Office of the
Privacy Commissioner
of Canada

Privacy and Your Reputation
Who Shapes Your Identity Online?

Annual Report to Parliament 2012

Report on the
Personal Information Protection and Electronic Documents Act

LOADING...

Privacy and Your Reputation

Who Shapes Your Identity Online?

Office of the Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 947-1698, 1-800-282-1376
Fax (613) 947-6850
TDD (613) 992-9190

© Minister of Public Works and Government Services Canada 2013

Cover image: Michael Rhodes, Paladin Design

Cat. No. IP51-1/2012E-PDF
1913-3367

This publication is also available on our website at **www.priv.gc.ca**

Follow us on Twitter: @privacyprivee

Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 947-1698
Fax: (613) 947-6850
1-800-282-1376
www.priv.gc.ca

Commissaire à la protection de la vie privée du Canada

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 947-1698
Téléc. : (613) 947-6850
1-800-282-1376
www.priv.gc.ca

June 2013

The Honourable Noël A. Kinsella, Senator
The Speaker
The Senate of Canada
Ottawa, Ontario K1A 0A4

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Personal Information Protection and Electronic Documents Act* for the period from January 1 to December 31, 2012.

Sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 947-1698
Fax: (613) 947-6850
1-800-282-1376
www.priv.gc.ca

Commissaire à la protection de la vie privée du Canada

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 947-1698
Téléc. : (613) 947-6850
1-800-282-1376
www.priv.gc.ca

June 2013

The Honourable Andrew Scheer, M.P.
The Speaker
The House of Commons
Ottawa, Ontario K1A 0A6

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada on the *Personal Information Protection and Electronic Documents Act* for the period from January 1 to December 31, 2012.

Sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

Table of Contents

Message from the Commissioner 1

About This Report 5

Privacy by the Numbers in 2012 6

Chapter 1 – Spotlight on Citizens: *Shaping Your Online Reputation* 7

1.1 Complaint Investigation: *Teen impersonated by phony Facebook account* 8

1.2 Complaint Investigation: *Profiles on PositiveSingles dating website turn up on other dating websites* 11

1.3 Investigation Update: *New owner of youth social networking site pledges to address all privacy concerns* 17

1.4 Advancing Knowledge on Online Privacy 18

Chapter 2 – Spotlight on Business: *Why the Buck Stops with You* 21

2.1 Accountability Guidance 22

2.2 Commissioner-initiated Complaint Investigation: *Rental company Aaron's uses spyware to recover laptop computers* 23

2.3 Complaint Investigation: *Insurer uses credit ratings to set premiums; clients in the dark* 25

2.4 Complaint Investigation: *Mortgage firm collects couple's personal information without knowledge or consent* 27

2.5 Complaint Investigation: *Insurance agent leaves sensitive information on voicemail* 29

2.6 Complaint Investigation: *Banker errs in sharing husband's data with wife* 30

2.7 Collaborative Complaint Investigation: *WhatsApp Messenger moves to correct privacy risks in mobile app* 31

2.8 Complaint Investigation: *Telecom company fails to adhere to its own policies on requests for access to personal information* 34

2.9 Complaint Investigation: *Summer camps trade information on child without parent's consent* 37

2.10 Complaint Investigation: *Store camera no longer captures neighbour's yard* 38

2.11 Data Breaches 39

2.11.1 *LinkedIn moves quickly to stem damage from major cyber-attack* 41

2.11.2 *Investor services employee responds to phishing e-mail* 42

2.11.3 *Password information stolen with laptop computer* 42

2.12 Update on Google's Privacy Policy: *Concerns about linking and retaining data remain* 42

2.13 Compliance Audit Update: *Independent authority confirms Staples addressed privacy concerns* 43

Chapter 3 – Spotlight on Us: *Responding to Your Privacy Preoccupations* 45

3.1 Information Centre 46

3.2 Complaint Intake 46

3.2.1 Written Submissions Received 47

3.2.2 Complaints Accepted by Industry Sector 48

3.2.3 Types of Complaints Accepted 49
3.3 Early Resolution of Complaints 49
3.3.1 *Utility company curbs collection of personal data* 50
3.3.2 *Foreign retailer swaps SIN for PIN* 50
3.3.3 *Insurance firm purges old records to comply with retention rules* 51
3.3.4 *Company retrains staff to handle privacy queries* 51
3.4 Serving Canadians Through Complaint Investigations 52
3.5 Advancing Knowledge 53
3.5.1 Contributions Program 53
3.5.2 Research on Web Leakage 55
3.5.3 Understanding Predictive Analytics 57
3.5.4 Online Direct-to-Consumer Genetic Testing 57
3.6 Engaging with Business 58
3.6.1 The Toronto Office 58
3.6.2 Business Survey 59
3.7 Guidance, Policies and Tools 60
3.7.1 Policy on Online Behavioural Advertising 61
3.7.2 Guidance on Cloud Computing for SMEs 62
3.7.3 Privacy Emergency Kit 63

Chapter 4 – Spotlight on Institutions: *PIPEDA and the Evolution of Privacy Rights* **65**
4.1 In Parliament 67
4.1.1 *Commissioner testifies at hearings on social media and privacy* 67
4.2 In the Courts 69
4.2.1 *Privacy Commissioner of Canada v. Association of American Medical Colleges* 69
4.2.2 *X v. The Toronto-Dominion Bank et al* 70
4.2.3 Judicial review applications: *X v. Privacy Commissioner of Canada* 71
4.2.4 Judicial review application: *X v. The Attorney General of Canada and the Privacy Commissioner of Canada* 71
4.2.5 Supreme Court of Canada Intervention: *X. v. Bragg Communications Inc.* 71
4.3 Substantially Similar Provincial and Territorial Legislation 73
4.4 Collaborating with Provincial and Territorial Counterparts 74
4.5 Global Initiatives 75
4.5.1 Co-operative Enforcement 75
4.5.2 Other International Activities 76

The Year Ahead **79**

Table of Contents

Appendix 1 – Definitions **83**
Definitions of Complaint Types under PIPEDA 83
Definitions of Findings and Other Dispositions 84
Investigation Process 86

Appendix 2 – PIPEDA Investigation Statistics for 2012 ..... **88**
Complaints Accepted by Industry Sector 88
Complaints Accepted by Complaint Type 90
Complaints Closed by Industry Sector and Disposition 91
Investigations Closed by Complaint Type and Disposition 92
Average Treatment Times by Disposition 93
Average Treatment Times by Complaint and Resolution Types 94
Voluntary Breach Notifications by Industry Sector and Incident Type 95

About PIPEDA

The *Personal Information Protection and Electronic Documents Act*, or PIPEDA, sets out ground rules for the management of personal information in the private sector.

The legislation balances an individual's right to the privacy of personal information with the need of organizations to collect, use or disclose personal information for legitimate business purposes.

PIPEDA applies to organizations engaged in commercial activities across the country, except in provinces that have substantially similar private-sector privacy laws. Quebec, Alberta and British Columbia each have their own law covering the private sector. Even in these provinces, PIPEDA continues to apply to the federally regulated private sector and to personal information in inter-provincial and international transactions.

PIPEDA also protects employee information, but only in the federally regulated sector.

Message from the Commissioner

As the *Personal Information Protection and Electronic Documents Act* approaches its teen years, it seems appropriate to contemplate the astonishing changes in the privacy landscape that surrounds it.

When the law that is the subject of this annual report to Parliament was passed in 2000, "phishing" was done in lakes, an "app" was served before dinner, and "friending" was not a verb. Online shopping was a novelty and Internet banking was in its infancy. In waiting rooms and at bus stops, thumbs were twiddled; they didn't flutter across tiny screens.

But for all the marvels and conveniences of the digital age, there are undesirable elements as well. The frauds and online swindles. The data breaches of sometimes colossal proportions. The capacity for covert, even malicious, probing into the lives of others. Cyberbullying and the potential to ruin reputations with ease and anonymity.

Amidst these frenetic changes, the protection of privacy is not child's play. It demands a law that is strong and mature, nuanced and effective. PIPEDA, conceived in another millennium, is no longer up to the task.

This is not to say that we haven't had some sterling successes over the first dozen years. Investigations and audits of online titans such as Facebook and Google, retail giants such as Winners and Staples, big businesses from Air Canada to CIBC, and hundreds of smaller organizations, have helped mould and nurture the privacy rights of Canadians.

To what can we attribute such success? I have to pay tribute here to Canadian citizens who have taken the time to bring privacy issues to our Office, to our staff who have spared no effort in addressing their concerns, and to the business community itself. For the most part, enterprises doing business in Canada understand the value of privacy and recognize its importance to customers. Indeed, it is gratifying to see the progress we have made in clarifying notions of consent, accountability, transparency and other fair information principles enshrined in PIPEDA today.

And yet, at the same time, it is very disheartening to see major Canadian organizations still demonstrating systemic carelessness in privacy protection—as some of our case studies show. In others, it's painfully clear that successful resolutions come only after considerable and even exhaustive, uses of resources and time.

As this report makes clear, we may have gone as far as we can with the current law, which has evolved little from the day it was passed.

Burgeoning challenges

Today's reality is that life online, new data-mining technologies, demands from law enforcement authorities for digital evidence, a host of new cyber-threats, and contemporary cloud-based business models all call for dramatically reformed approaches to the protection of personal information.

These are global challenges that must be met with global solutions. We need to collaborate with our international counterparts, but collective action works best when all jurisdictions work from a similar footing.

But with PIPEDA, that is no longer the case; we have fallen too far behind. While other nations' data protection authorities have the legal power to make binding orders, levy hefty fines and take meaningful action in the event of serious data breaches, we are restricted to a "soft" approach: persuasion, encouragement and, at the most, the potential to publish the names of transgressors in the public interest. In many cases, our work results in companies adopting more privacy-friendly practices, but usually at great expense, both in terms of time and resources. And, when push comes to shove, short of a costly and time-consuming court battle, we have no power to enforce our recommendations. All told, stronger enforcement measures in PIPEDA would provide incentives for organizations to take their responsibilities more seriously in the first place and build in privacy protections up front, knowing that the financial consequences of breach under a stronger regime could be real and significant.

PIPEDA today stands at a critical juncture. As with many teens, it's time to chase it off the couch so it can face up to bigger responsibilities.

* * *

I, too, am at a juncture, with my mandate coming to an end just a few months from now. After 10 years as Privacy Commissioner, this will be the last PIPEDA annual report that I will present to Parliament.

As I look back over the past decade, I feel a sense of pride at the accomplishments of our Office and the talented people it has attracted. I have had the extraordinarily good fortune to be surrounded by people skilled in investigations, compliance audits, policy development, technology, research, public education and the law, and truly devoted to the privacy rights of Canadians.

Gratifying too are the changes I have seen among Canadian organizations and individuals.

Our most recent public opinion polling suggests that Canadians have grown increasingly aware of the sanctity of their personal information. Most now recognize the potential perils of posting contact data or information about their whereabouts online, or submitting personal data to websites they suspect are sketchy.

Multiple responsibilities

Better yet, people seem to understand that they themselves play a leading role in safeguarding their personal information and online identity. Indeed, our survey, conducted toward the end of 2012, revealed that a healthy majority have decided against installing an app, or have uninstalled one, on the grounds that it asked for too much personal information.

Our Office has worked hard to reinforce such messages in the public mind. In that context, a key theme explored in this annual report relates to identity in the online universe and, more specifically, the importance of controlling one's own reputation on social media. Among other things, you will find here reference to some information pieces we published for individuals last year, as well as summaries of investigations we conducted on Facebook; Nexopia, a social network geared toward youth; and PositiveSingles, a dating network for people with sexually transmitted diseases.

But people can only take responsibility for their online activities if enterprises enable them to. That's why our outreach activities, our work in the courts, our international efforts and other activities over the years have aimed to persuade business that they need to step up with meaningful privacy management programs, understandable policies on the handling of personal information, and effective data-protection practices at all levels of the organization.

Under PIPEDA, companies are accountable for the personal information they collect, a second key theme of this report. You will read here about our new *Accountability Guidelines* and guidance we issued on a range of other technologies and business practices, LinkedIn's efforts to mop up after a significant data breach, and a groundbreaking international investigation into the WhatsApp Messenger service.

If individuals and organizations are prepared to play their respective roles in privacy protection, then government ought to support their efforts. There is no doubt in my mind that the privacy challenges of tomorrow will only continue to balloon, overwhelming—sooner or later—the capacity of the current law to respond.

And so, as I move on from my position as Privacy Commissioner, I can only hope that my successor will see PIPEDA revitalized, for the benefit of businesses operating in Canada, and all Canadians.

Jennifer Stoddart
Privacy Commissioner of Canada

About This Report

As the *Privacy by the Numbers* chart attests, 2012 was another active year for our Office. This Annual Report elaborates on these and many other activities we undertook on behalf of Parliament, stakeholders and the Canadian public.

Throughout the year, we kept our eyes firmly on our mission to guide Canadians toward greater privacy and protection of their personal information. We did this in several different ways, which are reflected in the division of chapters in this report.

Chapter 1: *Spotlight on Citizens* highlights a key theme that we noticed emerging from our investigative and other work in 2012. Entitled "Shaping Your Online Reputation," the chapter describes the threats to people's identities and reputations that lurk in the online world, and what our Office has done to help Canadians recognize and address them.

Chapter 2: *Spotlight on Business* elaborates on the idea that enterprises are accountable for the personal information of customers that they collect, use, hold and disclose. Called "Accountability: Why the Buck Stops with You", the chapter illustrates the point through summaries of key complaints we investigated in 2012, as well as noteworthy data breaches that were reported to us. The chapter also describes the guidance we issued on the topic of accountability.

Chapter 3: *Spotlight on Us* is dubbed "Responding to Your Privacy Preoccupations" because it highlights the concerns that prompted Canadians to call our Information Centre or file complaints with our Office. The chapter summarizes the work we did to address those concerns, including our ongoing emphasis on resolving issues in a timely and effective manner. The chapter also showcases the privacy-related research we either fund externally or conduct ourselves, and how this informs our guidance for organizations, information products for individuals, and so many other aspects of our work.

And finally, ***Chapter 4: Spotlight on Institutions*** focuses on our efforts to strengthen Canada's private-sector privacy law. Entitled "PIPEDA and the Evolution of Privacy Rights", the chapter reports on our engagement with Parliament and the legal system, as well as our work in reinforcing privacy protections for Canadians in concert with provincial, territorial and international privacy authorities, and other global organizations.

Privacy by the Numbers in 2012

PIPEDA Information Requests and Complaints		
Information requests received		4,474
Complaints accepted for formal investigation		220
Formal investigations closed		
Investigations satisfactorily concluded	140	145
Investigations deemed well founded and unresolved	5	
Complaints accepted for early resolution		138
Early resolution complaints closed		115
Early resolution complaints transferred for formal investigation		23
PIPEDA Breach Notifications		
Accidental disclosure	9	33
Loss	3	
Theft and unauthorized access	21	
Parliamentary Affairs*		
Bills and legislation reviewed for privacy implications		14
Parliamentary committee appearances		10
Formal briefs submitted		3
Other interactions with Parliamentarians or staff (for example, correspondence with MPs or Senators		57
Stakeholder and Public Relations*		
Speeches and presentations delivered		101
Tools, policy and guidance documents issued		7
Contribution agreements signed		11
Visits to main Office website	1,950,086	2,923,759
Visits to Office blogs and other websites (including the OPC blog, youth blog, youth website, deep packet inspection website and *YouTube* channel)	973,673	
Tweets sent		1,012
Twitter followers as of Dec. 31, 2012		5,130
Publications distributed		18,186
News releases and announcements issued		29

* Unless otherwise specified, these statistics also include activities under the *Privacy Act*, which are described in a separate annual report

Shaping Your Online Reputation

Many of us invest a fair bit of effort in reflecting on who we are and how we want others to perceive us.

As kids we dress up as princesses or superheroes. In preparation for our first date, we implore the mirror to declare us suave, sexy or cool. Later, as we navigate the adult world, we methodically groom and project an image of our choosing—the skillful carpenter, the caring nurse, the knowledgeable realtor, the trustworthy shopkeeper.

In the online universe, however, image and identity are more fluid and fragile. In a world where words are cheap and pictures can be posted with care or with malice, a reputation can be burnished and tarnished with equal ease.

Whether this is good or bad is a matter of personal taste and sensibilities. But, for us in the privacy business, the core issue is surely one of personal control.

We take the view that people have a right to shape their own reputations, to be who they want to be online. But that demands that websites be transparent about their operations, so that individuals who use them can understand, make choices and express their consent about the handling of their personal information.

In this chapter

As this chapter reveals, however, things are not always as they should be. There's the case of the Facebook profile that doesn't belong to the person in the picture; it's a nasty fake, posted by an imposter.

There's also the dating website for people with sexually transmitted diseases, whose database turns out to be a glass box: You drop your personal information inside, and it's visible from dozens of other dating pages you'd never guess were part of the same network.

The chapter also explores such timely issues as youth privacy and describes research that we have commissioned or funded to better understand reputational management in the online world.

1.1 COMPLAINT INVESTIGATION: *Teen impersonated by phony Facebook account*

Background

In 2012 we investigated a case in which a young teen fell victim to a Facebook impersonation. Even though the girl had never had a Facebook account of her own, somebody else set one up in her name.

The fake account looked real enough. It included a picture of the 13-year-old, prompting some of her real friends to connect with the account—or "friend" her, as they say in Facebook parlance. The imposter then reached out to those new contacts with inappropriate comments that appeared to have come from the girl.

As soon as the teen discovered that she had been impersonated on the social network, her mother contacted Facebook by e-mail and demanded that the organization immediately and permanently delete the imposter account, along with all comments attributable to it. She also demanded that the company contact the fake profile's so-called "friends" to inform them of the deception.

The mother also complained to our Office, alleging that Facebook Inc. had violated its own *Statement of Rights and Responsibilities* when it allowed an imposter to set up a Facebook account in the girl's name.

What we found

Our investigation determined that Facebook has a process to report phony accounts, which is described in its Help Centre. The reporting process is accessible to people with a Facebook account as well as those without.

Once an account is found to be false it can be disabled, and all posts and messages sent from the account are immediately removed from the social networking site.

Facebook confirmed to our Office that it had invoked this process to permanently delete the imposter profile and associated content, including all comments that had been posted from it.

The company also stated that, within five days of determining that the account was a fake, it had deleted from its systems the personal data provided by the complainant, in accordance with its policy to delete or destroy personal information no longer required for the purpose of its collection. The mother had furnished her daughter's passport photo and other identity information, so that Facebook could confirm that the imposter account really had been fake.

However, with respect to the complainant's expectation that Facebook notify the phony profile's "friends" about the deception, Facebook informed us that, as a matter of general policy, it does not send

such notifications on behalf of users, and had not done so in this instance.

The company argued that it would be inappropriate and impractical to notify the "friends" linked to an impersonated account. The company stated that it is a platform provider, and therefore a third party to online interactions. It is not Facebook, but individuals, who transmit personal information—whether accurate or false.

As a practical matter, Facebook also stated that, once an account is disabled, all posts and messages sent from the account are removed from Facebook immediately. If an imposter or otherwise abusive account holder has sent messages to other Facebook users, those messages are no longer available in the system as soon as the account has been disabled.

Facebook further took the view that it cannot always ascertain which user issues are legitimate and which ones are not. If there is a request to disable an account, Facebook can verify the identity of the requestor and act on an uncontested request. However, even at that, Facebook said it is not in a position to confidently state that an account is being disabled for reasons of impersonation.

For these reasons, Facebook argued that it is best to leave it to individuals themselves to take action against imposters in the manner they deem appropriate.

The company also made the point that if it got involved in notifying the "friends" of an impersonated account, the intervention itself could escalate or inflame the situation, potentially leading to further victimization of the impersonated individual.

Under PIPEDA, we found there was no requirement for the organization itself to notify individuals "friended" by an imposter account because this would require Facebook to intervene in interpersonal relations and arbitrate on what is true or not.

Further concerns

However, while PIPEDA may not oblige Facebook to notify the "friends" linked to an imposter account, we remained deeply concerned for the reputational and emotional fallout that victims of impersonation could suffer on social network sites.

We accepted that Facebook users could use the platform to correct misinformation about themselves from their own accounts, and reinstate their online reputation in their own words and on their own terms. Even so, we remained concerned for people who are *not* on Facebook, and therefore have no way to identify or contact the deceived "friends" to set the record straight.

And so we emphasized the need for Facebook, particularly in cases involving non-users, to take more responsibility for its business model, which allows imposter accounts to occur in the first place. We encouraged the company to help address or mitigate the emotional and reputational damage resulting from such privacy-infringing occurrences.

After eight months of consultations with our Office, the company ultimately agreed to implement a new

process whereby it would examine and investigate, on a case-by-case basis, instances in which the alleged impersonation of non-users is brought to its attention and the apparent victim requests assistance.

Although Facebook would not itself send notifications to the "friends" of an imposter account to advise them of a deception, the company offered to facilitate a process whereby non-users could themselves notify people "friended" by the imposter account, in order to restore their own online reputation. We felt that this measure would help put non-users on an equal footing with users.

In the particular case of this complaint, however, the imposter account and related information had been promptly deleted, so Facebook could offer no further assistance of this nature.

We concluded that Facebook had acted properly by promptly deactivating and deleting the imposter account.

Final thoughts

Information in the online universe is highly pervasive and accessible. It is generally also persistent, outlasting all but the most determined efforts to purge or control it. When such information is damaging or wrong, it can pose a grave threat to a person's privacy and reputation—online as well as in the physical world.

Given the magnitude of the risk, the protection of personal information online has to be the responsibility of everyone—data protection authorities, organizations and individuals alike.

Indeed, this case underscores the importance of educating youth and parents about the potential misuses of Internet technology. It reminds us to be vigilant about online information about us, and to move swiftly when information is false, abusive or otherwise damaging. The longer incorrect information remains online, the more harmful it can be to people's reputations.

In furtherance of this point, our Office was granted leave to intervene in another case of cyberbullying that was heard by the Supreme Court of Canada in 2012.

The case, involving a 15-year-old victim, raised a variety of issues that are strategic priorities for our Office, including identity integrity, youth privacy, the privacy risks associated with social networking sites, and the need for established social norms and legal rules to adapt to the Internet age.

As we report more fully in Chapter 4, we presented written and oral arguments elaborating on the legal framework that courts should consider when weighing privacy rights against the principle of open courts.

New Privacy Resources for Youth

We continued in 2012 to develop new resources to help children and young people face online privacy challenges.

In particular, we unveiled a presentation package for students in Grades 4 to 6, complementing presentations we had previously launched for Grades 7 and 8 (Secondary I and II in Quebec), and 9 to 12 (Secondary III to IV in Quebec). These packages help parents, educators and community leaders offer engaging and effective presentations to youth on the impact of technology on privacy, and the skills needed to build a secure identity online.

We also launched a graphic novel entitled *Social Smarts: Privacy, the Internet and You*, illustrating how to recognize and control the privacy risks associated with social networking, mobile devices and texting, as well as online gaming.

Social Smarts: Privacy, the Internet and You (http://www.youthprivacy.ca/en/gn_eng.pdf)

And we held our fourth annual *My Privacy and Me* student video contest, attracting entries from students across the country.

Our efforts to promote the distribution of our youth privacy resources were well received and gained even greater attention. Articles highlighting the graphic novel, presentation packages and our youthprivacy.ca website were featured in teachers' publications in Ontario and New Brunswick; the Canadian Association of School Libraries' journal, *School Libraries in Canada* (*SLIC*); and *Canadian Teacher Magazine*.

By the end of the year, we had received more than 170 requests for graphic novels, with requests originating from each and every province and territory across Canada.

1.2 COMPLAINT INVESTIGATION: *Profiles on PositiveSingles dating website turn up on other dating websites*

Background

PositiveSingles.com is an online dating website for people with sexually transmitted diseases. We received a complaint from several people who alleged that PositiveSingles had disclosed their personal information without their knowledge and consent.

The complainants said that, in setting up their online profiles, they provided sensitive personal information. They said they felt comfortable doing so because they were led to believe that the information would be protected. Their belief was reinforced by a statement on the PositiveSingles homepage that indicated that the organization does not "disclose, sell or rent any personally identifiable information to any third-party organizations."

After becoming members of PositiveSingles, however, the complainants discovered that their profile pictures and highly sensitive medical and other personal information that they had provided

PositiveSingles began showing up on what appeared to be numerous other dating websites. Many of those websites targeted people with varied interests and from different demographics, often with entirely different medical conditions.

For example, one of the complainants showed us that her personal profile appeared on 57 other social networking websites. Some of those were explicitly designed to appeal to people with specific sexual preferences or communicable conditions, or those seeking casual sex — descriptors that she said did not correspond at all with the profile she had posted on PositiveSingles.

The complainants contended that PositiveSingles had failed to inform them that the other sites existed, to obtain their consent for the sharing of personal information with other sites, and to provide an opt-out option.

Moreover, the complainants claimed that when they realized how their information had been shared with other sites, they asked PositiveSingles on numerous occasions to remove their personal information from those sites but the website did not comply.

They therefore filed a complaint with our Office against both PositiveSingles and its owner, SuccessfulMatch.

What we found

California-based SuccessfulMatch, which owns and operates PositiveSingles.com, is a business centre for potential web entrepreneurs who wish to set up affiliate websites. Both PositiveSingles.com and SuccessfulMatch.com list a Toronto-area address and telephone number.

According to its homepage, PositiveSingles claims to be the "best, largest, completely anonymous and most trusted online dating site for people with Herpes, HPV, HIV / AIDS, Hepatitis, Chlamydia, Gonorrhea, Syphilis and other STDs in the world."

SuccessfulMatch, for its part, has numerous other web-based dating networks within its operations, typically catering to specific demographics and interests. When a third party, such as an Internet entrepreneur, purchases a domain name for a particular dating network, SuccessfulMatch sets up an affiliate website for that domain and hosts the site.

SuccessfulMatch is responsible for activities related to the affiliate site, including the dating software, membership database, payment processing and customer support. The organization further informed us that an affiliate can only view the homepage of its own domain; it has no access to or control over any customer's profile or personal information, whether on its own affiliate site or on the main network site. Our investigation found no evidence to contradict this.

SuccessfulMatch told us that affiliated websites are effectively "extensions" of the main dating network and serve as "doors" to the same community.

For the PositiveSingles network, "PositiveSingles.com" is the main site, and also maintains the membership database for this and all affiliate sites within the PositiveSingles network. PositiveSingles is also said to "power" the various affiliated websites, although we found that the websites offered no clues as to how this happens or what it means. Indeed, we could not determine how many affiliates there were and what they represented, and SuccessfulMatch advised us that the numbers are in constant flux as sites are set up and taken down.

We explored these relationships to determine whether SuccessfulMatch disclosed the complainants' personal information to third-party websites as the complainants alleged. They felt that the very fact that their profiles appeared on numerous other sites pointed to an improper disclosure.

In fact, although the domain names of the affiliate sites are owned by third parties, an affiliate does not collect any information, and has no access to or control over, the affiliate site associated with its domain name. SuccessfulMatch, for its part, collects and controls the information in its database.

Our investigation therefore established that SuccessfulMatch did not disclose the information to an outside third party; rather it used the information coming through the affiliate sites (and its own PositiveSingles.com site) to generate a single, all-encompassing database.

As such, our investigation focused on whether SuccessfulMatch obtained adequate consent for the use of the complainants' information in this manner, whether the information was sufficiently well safeguarded, and the use of cookies on the site.

Our conclusions

- **Consent**

The PositiveSingles.com homepage features a prominent button labelled "How we protect your privacy." It leads to a page filled with unqualified assurances of privacy and confidentiality for members of the site. We felt that a user could easily mistake this for the site's privacy policy, even though SuccessfulMatch was using it as a marketing tool to attract people who, by virtue of their medical conditions, would place a high premium on privacy.

The actual *Privacy Policy* and *Service Agreement*, which must be read together in order to appreciate potential privacy implications, were found as small-font hyperlinks at the bottom of the homepage and the "How we protect your privacy" page. Those documents, moreover, do little to clarify what happens to the personal information of people who become members of PositiveSingles.

Indeed, since PositiveSingles appeared to be, and was presented as, a standalone site, prospective members would not ordinarily conclude that their profiles would be used by a network of affiliate sites, or incorporated into a broader database.

In short, we found that PositiveSingles projected an outwardly caring attitude that could foster a reasonable expectation of enhanced protection for

members' sensitive personal information. By contrast, however, this personal information was made widely available for use by a network of websites that could change daily—without the knowledge of the members concerned.

We concluded that it was not possible for an individual to reasonably understand how their personal information might be used or disclosed. We therefore concluded that SuccessfulMatch failed to uphold the openness principle of PIPEDA, and that consent obtained from prospective users for the use of their personal information could not be considered meaningful.

- **Safeguards**

Given the sensitivity of the medical and other personal information of members of PositiveSingles, confidentiality is critical. It is essential that members' personal information be protected and confined to a population of other people that the members know about and approve of.

The complainants, however, furnished evidence that some members' personal information could be accessed by non-members via simple searches on a common search engine. This suggested that proper safeguards were not in place, another violation of PIPEDA.

However, we subsequently observed that member profiles or nicknames did not appear in blog posts of the Internet search engine's cache, which indicated that there may have been efforts to address this issue.

- **Cookies**

Web cookies are small bits of computer code that third parties, such as advertisers, place on the computers of Internet users, in order to gain valuable information about the computer or its user. Cookies may be used for a variety of purposes, such as tracking the preferences or browsing practices of individuals, sometimes with the goal of targeting them with tailored advertising content.

Our investigation determined that the *Privacy Policy* for PositiveSingles provides basic details about its use of cookies and how an individual can disable the function. The policy also states that third-party advertisers may place or read cookies on a user's browser.

We noted that there was no information on the type of cookies used, or whether the cookies enabled the sharing of personal information.

While PositiveSingles' website pledged that the organization would "never sell your profile to any third-party entity like many other sites do," SuccessfulMatch suggested in its *Privacy Policy* that it may engage in online behavioural advertising—a practice that could use cookies to track the preferences and browsing activities of website users.

We took the position that, if SuccessfulMatch was, in fact, engaging in online behavioural advertising, then it had to obtain meaningful consent from the people who were being tracked and targeted. Our Office's guidelines on the practice further state that, if the tracked individuals have certain highly sensitive

medical conditions, then the consent must be express, not implied. People must actually opt in to the use of their personal information for such a purpose.

Our recommendations

In a preliminary investigative report, completed in October 2012, we made the following recommendations to SuccessfulMatch:

- Users should know upfront that their profile information will be included in a database that will be accessed by other online dating websites that are affiliated with PositiveSingles and that target specific medically and demographically diverse populations. Moreover, they should be advised that they will not be able to know which sites those are, and they will not be able to remove their profiles from them.

  The website's privacy policy should explain how information is used by SuccessfulMatch through its affiliate sites.

- The relationship between SuccessfulMatch.com and PositiveSingles.com should be made clear, prominent and explicit to users.

- The distinction between "third-party" sites and "affiliate" sites should be made clear, prominent and explicit for users.

- We also recommended that SuccessfulMatch provide our Office with detailed information on how the personal information of registered members is safeguarded on PositiveSingles, including any technical measures and protocols used to prevent hacking and to keep non-registered individuals from viewing personal information published on the site and its affiliate sites.

- We also asked for details on SuccessfulMatch's uses of web cookies. If the cookies are used to track online behaviour for the benefit of third-party advertisers, then the site must give individuals the opportunity to provide or withhold their express and informed consent.

What happened next?

SuccessfulMatch responded to our recommendations with the following actions:

- The organization changed the homepage and registration page of the PositiveSingles website to indicate that all profiles created on PositiveSingles.com become visible to users of other affiliate websites in the PositiveSingles network.

- Although profile information is visible on other affiliated websites within each network operated by SuccessfulMatch, the organization confirmed that is does not share profile information between its various networks. It amended its *Service Agreement* accordingly.

- The *Privacy Policy* and other areas of the SuccessfulMatch website were changed to better explain the relationships between SuccessfulMatch, PositiveSingles, and

the broader "family of businesses which ...includes many other websites...."

- The *Privacy Policy* was amended to include clear definitions and to better explain the nature and function of affiliate sites, and how they relate to PositiveSingles and SuccessfulMatch.

- The *Privacy Policy* for PositiveSingles was also reworded to clarify the difference between "third-party" sites and "affiliate" sites.

- SuccessfulMatch informed us of the safeguarding measures it uses to protect members' personal information, including to prevent user data from being accessible to search engines. These measures include password verification, monitoring of user log data, firewalls and encryption.

- SuccessfulMatch amended its *Privacy Policy* to more clearly explain the purposes for which it uses cookies. The organization informed our Office that it does not permit advertising on its site, does not use cookies for behavioural advertising, and does not provide cookie information to advertisers.

We believe that these changes to the PositiveSingles site are important. Through greater transparency, users will be able to make more informed decisions before consenting to the use of their personal information on the PositiveSingles network of sites. That, in turn, will give them greater control of their online reputation.

Accordingly, we deemed the complaint to be ***well founded and resolved***.

Canadians leery about posting personal information online, poll finds

A survey of Canadians that our Office commissioned in late 2012 found that many people are very concerned about posting information about themselves online. Indeed,

- 55 percent said they had serious reservations about publicizing their location on the Internet,
- about half were concerned about posting contact information or personal photos or videos and
- more than four in 10 were apprehensive about sharing information about their social activities.

While only one in eight respondents overall said that they had experienced an online posting that had negatively affected their lives in some way, the proportion who reported they had been harmed by something they or someone else had posted about them was more than double (26 percent) among younger respondents aged 16 to 24. Young people tend to be heavier users of technology and are often less inhibited in the online universe than their parents or grandparents.

The survey, the latest in a series to take the pulse of Canadians on privacy, was published in the spring of 2013. More details will be included in next year's annual report.

1.3 INVESTIGATION UPDATE:
New owner of youth social networking site Nexopia pledges to address all privacy concerns

Our three-year-old investigation into complaints about a Canadian youth-oriented social networking site continued to elude a final resolution in 2012 while we took the matter to court, only to find the company being put up for sale in mid-action. Since the new owner has undertaken to adopt all of our recommended actions, however, we are hopeful for a resolution in 2013.

Our 2011 Annual Report highlighted the results of an in-depth investigation into the privacy practices of Nexopia.com.

Founded in Edmonton in 2003, Nexopia distinguishes itself from Facebook and later arrivals on the social networking scene by positioning itself as an "open community" of users who can "communicate with their online friends and 'show off' to the world."

Prompted by a complaint from the Ottawa-based Public Interest Advocacy Centre, our investigation found that Nexopia was in breach of PIPEDA in several respects. We made 24 recommendations for corrective action.

Twenty of those recommendations dealt with issues related to the disclosure of user profiles to the public; default privacy settings; the collection, use and disclosure of personal information collected at registration; the sharing of personal information with advertisers and other third parties; and the retention of personal information of non-users.

Nexopia committed to implementing 20 of these recommendations, the majority of them by June 30, 2012 and the remainder by Sept. 30, 2012. Accordingly, we deemed those findings to be ***well founded and conditionally resolved***.

However, Nexopia refused to adopt the remaining four recommendations, or to offer acceptable alternatives. Those recommendations related to the company's indefinite retention of users' personal information, even after a user had selected a "delete account" option, and to the absence of a mechanism to permanently delete personal information from the organization's archives.

We concluded that these matters were ***well founded*** and therefore remained unresolved.

Court Application

On April 13, 2012, our Office applied to the Federal Court, seeking an Order requiring Nexopia to cease retaining personal information indefinitely and to adopt a delete function that would allow for the permanent deletion of its website users' personal information, upon request and/or when the retention of personal information is no longer necessary for the fulfillment of the identified purposes for which it was collected. (*Privacy Commissioner of Canada v. Nexopia.com Inc.*, Federal Court File No. T-764-12).

On Sept. 30, 2012, Nexopia was sold to another company. The new owner undertook to address all 24 of our recommendations, by April 30, 2013.

At the time of this report's writing, we were in the process of assessing Nexopia's implementation of our recommendations.

Guidance for Gamers

Last September we released a fact sheet to help online gamers understand privacy settings and make informed choices when they're playing videogames over the Internet.

Gaming Consoles and Personal Information: Playing with Privacy (http://www.priv.gc.ca/information/pub/gd_gc_201211_e.pdf)

Entitled *Gaming Consoles and Personal Information: Playing with Privacy*, the fact sheet emerged from concerns we heard raised at our 2010 Public Consultations on Cloud Computing and Online Tracking. Academics and members of the public noted that there is very little advice available for people who enjoy playing online videogames.

And so we started looking into this burgeoning phenomenon. We tested game consoles and their privacy settings. We examined new features that tie game activity with social networks.

We ultimately came up with an FAQ (Frequently Asked Questions) for gamers young and old, as well as teachers and parents. We published our guidance document along with a learning plan on videogames that was developed for teachers tackling issues of online literacy in Canadian schools.

1.4 ADVANCING KNOWLEDGE ON ONLINE PRIVACY

Advancing knowledge on how to better promote and defend the right to privacy is one of our Office's key mandates. Over the years, we have developed a dynamic and forward-looking research strategy, both in-house and through our well-regarded Contributions Program.

Since 2004, the Contributions Program has funded groundbreaking work on a range of privacy-related issues. Here are specific projects we have funded through the program that touch on online privacy and its impact on people's reputations:

- "Young Canadians in a Wired World" is a long-term project by **MediaSmarts** (formerly known as the Media Awareness Network) that began in 2000. It tracks and investigates the behaviours, attitudes and opinions of Canadian children and

youth with respect to their use of online spaces. Phase III of the project, currently underway, includes a national survey of 6,000 young people, aged nine to 17, to explore their views of significant technological and social developments in the online universe. A key aspect is to examine how young Canadians manage their personal information, privacy and reputation in the wired world.

- ***L'Association sur l'accès et la protection de l'information (AAPI)*** produced an educational kit in 2012 to help junior high school students develop sound privacy practices when they post pictures and personal information online. The project presents tools and ideas to encourage youth to be cautious about their online reputation. The kit will also help teachers discuss online privacy and personal information protection in class.

The Contributions Program funded 11 projects in 2012-13 and we expect that some of these results will help shed further light on issues related to online privacy and reputation, especially with respect to mobile devices.

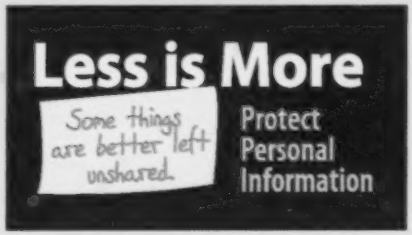
A more detailed description of the Program's activities in 2012 is contained in section 3.5.1 of this report.

Data Privacy Day

On Jan. 28, 2012 our Office joined governments, privacy professionals, corporations, academics and students from around the world in marking Data Privacy Day.

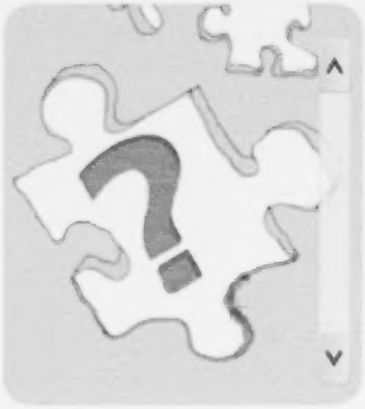
Our focus for this annual awareness-raising event was to encourage Canadians to restrict the amount of personal information they share online. By means of the slogan "Less is More: Some things are better left unshared", we aimed to help people curb their online exposure and, as a consequence, limit the risk that their personal information will be misused or disclosed without consent.

Businesses were also encouraged to think *less is more* when they collect and retain the personal information of customers. After all, the more information they have, the greater their risk of running afoul of PIPEDA.



Why the Buck Stops with You

On U.S. President Harry S. Truman's desk stood a sign that proudly pronounced: "The Buck Stops Here!" The man who led America through seven tumultuous years beginning in 1945 wanted the world to know that he was in charge. He was the boss and could make tough decisions. He was seen, in a word, as accountable.



When it comes to privacy, Truman's sign might carry a message for organizations too. In the dozen years since PIPEDA became law, there's still too much passing the buck. Too often, companies assume that building privacy policies, communicating them to staff, and ensuring they are absorbed and applied is somebody else's job. Or, if it's theirs, then it's an afterthought, secondary to the main business of operating the enterprise.

But it's not. Accountability is the first fair information principle set out in Schedule 1 of PIPEDA. In its most general terms, accountability demands that an organization be ethically responsible for its actions. In particular, that confers on businesses a legal obligation to protect the personal information in their hands.

Accountable organizations should have a tailor-made program to manage and protect personal information under their control. This chapter describes a comprehensive guidance document that we issued in 2012, along with our counterparts in Alberta and British Columbia that have substantially similar private-sector legislation. Entitled *Getting Accountability Right with a Privacy Management Program*, the document leads organizations through the steps necessary to build privacy into their operations

An effective privacy management program is something that organizations should do for their customers, for sure, but it's in their interest as well. Indeed, all too often we find ourselves investigating cases of companies that enraged their customers through a lackadaisical approach to privacy.

Surely that can't be good for business. It's time to stop passing the buck.

In this chapter

This chapter explores the notion of accountability for privacy—where it's worked, where it's failed, and what's being done to strengthen it.

It summarizes cases that we have investigated under PIPEDA that turned largely on questions of accountability for the appropriate handling of personal information. In one case, the investigation was carried out through an unprecedented collaboration with our counterpart in the Netherlands.

But we did more than just chase down transgressors; we also preached the gospel of prevention. After all, businesses that understand the rules are more apt to avoid privacy pitfalls.

And so this chapter begins with a summary of a new guidance document we issued this year to help business better navigate their responsibilities under PIPEDA.

2.1 ACCOUNTABILITY GUIDANCE

Under the Accountability principle of PIPEDA, organizations are required to accept responsibility for protecting the personal information they hold. This means having policies and procedures that promote good practices. Taken as a whole, these constitute a privacy management program.

But even though accountability is enshrined in Canadian privacy law, we continue to run into some pretty basic accountability problems. In our investigations, for example, it's often unclear who in the organization is responsible for privacy, and whether a company has ever updated its privacy policy.

More recently, we were also observing that some organizations weren't incorporating privacy protections into their products and services. Even when policies were in place, it looked as though program developers and technologists— whose work has a potentially huge impact on individuals' personal information—hadn't read them or appreciated their importance.

And so, to our disappointment, we continued to encounter some very fundamental privacy breaches, where moments of employee inattention or ignorance about good privacy practice led to entirely avoidable spills of personal information.

Getting Accountability Right with a Privacy Management Program (http://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.pdf)

That's why in the spring of 2012, our Office, along with our counterparts in Alberta and British Columbia, published *Getting Accountability Right with a Privacy Management Program*.

The *Getting Accountability Right* guidance document sets out what our three offices expect in terms of privacy programs. It outlines the need for organizational commitments and program controls. Because a privacy program should be dynamic and flexible to accommodate changing needs and risks, the guidance also stresses the need for ongoing assessment and revision.

Our work in this field has been informed by significant developments abroad. We and the Information and Privacy Commissioners of Alberta and B.C., Jill Clayton and Elizabeth Denham, have been participating in an international discussion on what it means to be an accountable organization. Led by U.S. business interests, the initiative also involves data protection authorities in Europe and North America.

Indeed, accountability has developed into a global privacy theme. The *Guidelines on the Protection of Privacy and Transborder Data Flows* of the Organisation for Economic Co-operation and Development were the first international document to include the concept three decades ago. The Privacy Framework developed by Asia-Pacific Economic Cooperation (APEC) also includes accountability, and the European Commission's proposed new privacy regulation incorporates the notion of "demonstrable accountability" in a very tangible way.

The quantities of personal information, the complexity of processing it, and the variety of privacy frameworks that exist in different countries, largely account for this broadening interest in the concept. Since Canada has long had the accountability principle enshrined in law, our three offices decided we would flesh out our perspectives and add our voices to the international conversation, with the goal of improving compliance on the home front.

The document has been well received, garnering discussion at the International Association of Privacy Professionals meeting in Brussels, along with the European-American Business Council in Washington D.C. A major national law firm and the Centre for Information Policy Leadership have also developed tools for clients and members based on the document.

2.2 COMMISSIONER-INITIATED COMPLAINT INVESTIGATION: *Rental company Aaron's uses spyware to recover laptop computers*

Background

In early 2012 we learned that rent-to-own companies in Canada were allegedly using a spyware application called Detective Mode to covertly trace missing laptop computers.

The software, supplied and supported by U.S.-based DesignerWare Inc., could be installed and remotely activated in leased laptops, where it was designed to surreptitiously collect keystrokes, contact information, screenshots, webcam photographs and other information. The data could be sent back to the

rental company to aid in the recovery of lost or stolen laptops.

In consultation with the U.S. Federal Trade Commission, the Commissioner determined that she had reasonable grounds to initiate a complaint against a Canadian franchisee of the large, publicly traded rent-to-own company Aaron's Inc. These grounds included credible evidence to suggest that the franchisee had requested the activation of Detective Mode on 30 occasions during a six-month period.

In our complaint, we alleged that a reasonable person would not consider that the recovery of missing computers justified the use of Detective Mode software. Moreover, we alleged that the indiscriminate nature of Detective Mode surveillance resulted in the collection of more information than necessary for the intended purpose.

What we found

Our investigation revealed that the Aaron's franchisee was no longer using Detective Mode. However, it had done so in the past for the purposes of laptop computer recovery.

The company claimed that its record-deletion practices made it impossible to determine the exact number of times Detective Mode was used. The franchisee did, however, confirm that it had requested at least five activations during a single week. The activations were prompted by the company's belief that the lessee had absconded with the laptop without making all the required payments.

The rental company stated that four of the five activations were successful in tracing the missing goods.

We found that the four successful activations resulted in the collection of hundreds of pages of records containing sensitive personal information. These included a webcam photograph of a user, as well as e-mail addresses, home addresses, phone numbers, and personal messages to family members and friends. There were also screen shots of social networking site pages that included pictures of children, as well as posted messages and other Internet content.

The data was surreptitiously collected using the laptop's webcam, recordings of user keystrokes, and even a fictitious operating system registration page.

None of the names and other contact details collected in this manner corresponded with names of the lessees who allegedly disappeared with the laptops. It is not known how these laptop users came into possession of the devices.

We concluded that the company's indiscriminate use of Detective Mode surveillance resulted in the collection of more personal information than required for the purposes of laptop recovery.

Moreover, things could have been still worse: Detective Mode is fully capable of capturing an

image of a child in her room, or the banking user ID and password of another innocent third party. When the software is activated, the rental company has no way to predict what information it will collect.

We appreciate the rental company's desire to protect its inventory, and that Detective Mode could, from a technological standpoint, be an effective tool in achieving this objective.

However, we found that the resulting loss of privacy was egregious and disproportionate to the rental company's potential financial benefit. Indeed, it is difficult to imagine a business objective that could justify this kind of indiscriminate and surreptitious collection of personal information.

What happened next?

Presented with our findings, Aaron's promised to delete all remaining personal information from its records as soon as possible. It also undertook never to use this kind of spyware again.

Consequently, we determined our complaint to be ***well founded and resolved.*** We will continue to monitor the Canadian market for the use of software of this nature.

2.3 COMPLAINT INVESTIGATION: *Insurer uses credit ratings to set premiums; clients in the dark*

Background

An Ontario couple was surprised when their property insurance premium increased substantially between policy renewals. They had had a perfect credit rating for 50 years, but this changed in one year when they co-signed a loan that resulted in three defaulted payments.

Their insurance company confirmed that a sudden change in their credit-derived score had, in part, negatively affected their home insurance premium.

The couple lodged a complaint with our Office, which we determined had three principal elements.

What we found

- **Purposes of collection**

For several years, the insurance company had been sending all its Ontario policyholders a detailed notice at the time of their first-year policy renewal. The notice explained how the company receives from a credit-reporting agency in Canada an insurance-related score that is derived from a policyholder's credit report, and how the insurance company may use the score as one of many factors in determining personal property insurance eligibility and premiums.

There is some indication that a credit-derived score is predictive of risk, although we found that this view is not unanimously held across the insurance industry.

With respect to this case, we concluded that a reasonable person would consider it appropriate for an insurance company to collect and use credit-derived scores as a tool to underwrite insurance policies and set premiums.

First, assessing risk through the use of reliable underwriting tools is a fundamental component of the insurance business. There is a benefit both for insurers, which can better manage risk and thus price their policies appropriately and competitively, and policyholders, whose premiums are better geared towards their particular level of risk.

Second, the practice is entirely lawful in Ontario. Section 8 of the province's *Consumer Reporting Act* states that credit information may be disclosed for the purpose of underwriting insurance. (The use of credit information in the property insurance context is not permitted in certain other provinces, including Newfoundland and Labrador.)

We further noted that the credit-derived score is an aggregate number, which may be less privacy intrusive than accessing an individual's entire credit report.

Consequently, we concluded that the complaint was ***not well-founded*** with respect to the purposes of collection.

It's also worth noting that the Insurance Bureau of Canada has issued guidelines concerning the use of credit information by insurers. The *Code of Conduct for Insurers' Use of Credit Information* steers insurance companies away from using credit information as a sole variable, and from denying quotes and insurance to customers who refuse to consent to the use of their credit information.

- **Consent**

As clients for six years, the couple were unaware of the insurance company's practice and felt that the organization did not have their express consent for the use of their credit information.

The insurance company, for its part, believed that the complainants consented to the collection of credit information when they signed their original application.

We found that the consent provisions on the insurance company's application form were not sufficiently precise to obtain meaningful consent for this use of credit-related information.

Nor could we expect customers to correctly surmise this use, since it is not a familiar or expected use of such information. Indeed, a survey commissioned by the Insurance Brokers of Ontario in November 2010 found that three-quarters of Ontario consumers were unaware that their credit scores were being used to determine how much they pay for their home insurance premiums.

We further noted that the insurance industry's own *Code of Conduct* provides detailed instructions for obtaining consent when using credit information and clearly advocates obtaining express and informed consent.

We did not see the insurance company's practice of sending more detailed information to policyholders one year after they had signed their initial policy as a means of obtaining proper consent.

Accordingly, we determined that adequate consent for the collection and use of such data had not been obtained. With respect to consent, we concluded the complaint was ***well founded***.

- **Openness**

The final element of the complaint related to the lack of explicit information available to individuals on how their personal information is used to determine premiums or eligibility.

Since the Ontario industry's own polling showed that three-quarters of Ontario consumers were in the dark about the potential use of their credit scores in the establishment of their home insurance premiums, it's not surprising that the complainants would say they were unaware of the practice.

Indeed, our investigation revealed that the company's website offered no explicit information about statistical scores or how credit score information is used to determine premiums. Nor was this information included in the company's privacy policy, which was available online.

We concluded that the complaint was also ***well founded*** with respect to openness.

What happened next?

In jurisdictions where it uses credit information as an underwriting tool, the company sent out a revised notice to all its policyholders. The objective was to inform customers about the firm's use of credit information to assess customer risk.

The company also updated its website to inform its insured clients that credit information is used as one of several underwriting tools to assess customer risk.

In response to our recommendations, the insurer also agreed to amend its application to include consent for the collection and use of the credit-derived scores. And it pledged to inform our Office when the consent language is amended.

We considered the complaint to be ***conditionally resolved*** and will follow up to ensure the full implementation of our recommendations.

2.4 COMPLAINT INVESTIGATION:
Mortgage firm collects couple's personal information without knowledge or consent

Background

A mortgage agent asked a mortgage company (acting as an administrator) to prepare a letter of interest for mortgage financing, containing a quote for a particular couple's financial capacity to build a home on their property. The company prepared the letter for the agent, but did so without the knowledge of the couple. The document was not signed by them.

To the couple's shock, the letter was later introduced in an ongoing court action that the couple had brought against one of their former spouses, who by then was remarried to the mortgage agent.

The letter contained significant amounts of personal information. Some of it had been taken from an affidavit that the couple had sworn and submitted at an earlier point in their court proceedings. Other information in the letter included the sales history of their property and personal funds available for construction.

The couple were particularly upset that the letter turned up in court because they were not clients of the mortgage agent or of the mortgage company, they were not looking for mortgage financing, and they had never requested such a letter.

Consequently, they filed a complaint with our Office.

What we found

A spokesman for the mortgage company told us that he had prepared the letter in good faith and had followed normal guidelines.

But he also admitted that he had taken the mortgage agent at his word and had not verified that the couple's consent had been obtained to collect, use and disclose their personal information for this specific purpose.

He also maintained that he was unaware that the letter might be used in court proceedings. However, he argued that some of the information about the couple was publicly available, and therefore exempt from PIPEDA's consent requirements.

We found that, in preparing and issuing the letter of interest for mortgage financing, the mortgage company collected, used and disclosed the couple's personal information without their knowledge or consent.

We also determined that, while some of the information did appear in the record of the ongoing court proceedings, the company could not assume that it was 'publicly available', and therefore exempt from PIPEDA's requirement to obtain consent for its disclosure.

PIPEDA's regulations state that personal information appearing in a public court record may only be considered 'publicly available' if *the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the record or document.*

In this case, we concluded that the purpose for which the mortgage company collected the personal information did not relate directly to the purpose for which the information appeared in the court record.

Consequently, the couple's consent should have been obtained for the collection, use and disclosure of the information in the letter.

What happened next?

In order to prevent a recurrence of such a situation, our Office recommended that the mortgage firm establish a procedure to obtain consent for the collection, use and disclosure of personal information. We also recommended that it keep us informed on how it would put the procedure into effect.

In response, the mortgage company established a new procedure under which personal information would not be collected, used or disclosed without the direct consent of the individual concerned. In situations where the personal information is obtained from a third party, the firm would examine the suitability of any pre-existing consent.

The company also trained its staff in the new procedure, and developed associated resource material.

Accordingly, we deemed the complaint to be ***well founded and resolved***.

2.5 COMPLAINT INVESTIGATION: *Insurance agent leaves sensitive information on voicemail*

Background

The complainant was employed by a hair salon when she telephoned her insurance company to obtain a quote for liability insurance for a home-based hair styling business she was planning to open. She was told that an insurance agent would call her back with the information.

A few days later, her employer retrieved a message from the salon's voicemail system, in which the insurance company was asking the complainant to call back with further details about her planned hairstyling business. When confronted by her employer, the complainant admitted that she planned to quit the salon in five weeks. She was dismissed within a week.

The complainant notified the insurance company of her firing, and asked why a detailed message had been left at her workplace, when she had asked to be called only at home. The company claimed they were unaware of any such request.

What we found

We found no evidence to corroborate the complainant's claim that she had specifically requested that the insurance company call her only at home. Nevertheless, there was no dispute between the parties that a message was left at the complainant's workplace.

The company, however, had no specific policy on leaving information on answering machines. When we suggested they create one, they initially refused.

In our view, the insurance company revealed more information than was necessary for the complainant to merely return the agent's call. We also felt that the message included sensitive personal information, and that it was vulnerable to interception by people other than the complainant.

Our investigation also determined that the insurance company's employees were required to sign a confidentiality agreement and abide by the provisions of PIPEDA. Within that context, we concluded that the agent should not have assumed that the complainant would have consented, even implicitly, to such sensitive personal information being left in such a public manner.

In our preliminary report we asked the company to develop policies to reduce the risk of disclosing clients' personal information to unauthorized third parties when leaving messages, and to provide privacy training to their privacy officer and employees.

What happened next?

In response, the insurance company pledged to implement a new procedure to minimize the amount of information left on telephone messages, and they provided us with sample communications.

The company also amended internal procedures, so that a client's contact information and messaging preferences are regularly updated.

Accordingly, we deemed the complaint to be ***well founded and resolved***.

2.6 COMPLAINT INVESTIGATION: *Banker errs in sharing husband's data with wife*

Background

In the course of a transaction, an employee of a bank mistakenly gave a customer a copy of a bank record containing her husband's detailed financial profile.

When the husband learned of the alleged disclosure from his wife, he complained to the bank as well as the Ombudsman for Banking Services and Investments.

Not satisfied with the responses he received there, he filed a complaint with our Office. He alleged that the bank disclosed his personal information to his wife without his knowledge and consent, and that the bank failed to safeguard his personal information.

What we found

The bank agreed that an employee disclosed the complainant's personal financial information without his consent to a person with no right to the information.

Our investigation determined that the bank had in place procedural safeguards that appeared to be

appropriate to the sensitivity of the complainant's personal information. Moreover, we found that the bank employee had recently completed training in customer privacy.

The employee, however, clearly failed to apply the bank's standard procedures to protect customer personal information. In particular, the employee disregarded the basic customer identification and authentication procedures, as well as a requirement that employees report any error or event involving customer information.

What happened next?

Following the incident, the bank coached the employees connected to this complaint on the importance of maintaining customer confidentiality, as well as on the bank's privacy policies and procedures.

Accordingly, we found the disclosure complaint to be ***well founded***. We found the complaint related to the bank's safeguards for personal information to be ***well founded and resolved***.

Final thoughts

This case demonstrates that security policies and procedures, though essential, are not in and of themselves sufficient to protect personal information from unauthorized disclosure. The effectiveness of security safeguards ultimately depends on their diligent and consistent implementation.

In view of repeated complaints about improper disclosures of personal information that we have received against the bank, we urged it to review and strengthen its employee training programs and internal governance.

In particular, we encouraged the bank to consult the guidance document *Getting Accountability Right with a Privacy Management Program* (see section 2.1), to ensure that what the bank mandates in its governance structure is actually implemented and executed within its organization.

2.7 COLLABORATIVE COMPLAINT INVESTIGATION: *WhatsApp Messenger moves to correct privacy risks in mobile app*

Background

WhatsApp's Messenger service is a smart phone application that allows people to exchange instant messages on their mobile devices using a data service (the Internet) rather than a telephone service. This feature distinguishes the service from the usual text or short-message services (SMS) commonly used on cellphones and smart phones. In addition to basic messaging, the application also allows users to send and receive images, video and audio messages.

WhatsApp's Messenger also allows users to communicate between different families of mobile

devices, whether they be BlackBerrys, iPhones, Windows-based phones or Androids—a feature generally not available on the proprietary messaging systems that manufacturers build into their own phones. However, both the sender and recipient of a message must have the application installed and registered with WhatsApp.

By early 2012 WhatsApp was one of the top-five best-selling mobile applications in the world, and was widely used by Canadians. By some estimates, more than one billion messages per day were transmitted by WhatsApp subscribers around the world.

Commissioner Stoddart, however, had some reasonable grounds for concern about the way WhatsApp Inc., the California-based company that operates the app, collected, used, disclosed and retained personal information. She initiated a privacy complaint in January 2012.

Meantime, the Dutch data protection authority, the *College bescherming persoonsgegevens*, also had some reservations about the privacy implications of the technology and consulted us on our views. Because of the international scope of the technology, and because international privacy issues increasingly demand an international response, we and the Dutch authorities decided to conduct separate but co-ordinated investigations.[1]

[1] For more information on this international collaboration, please refer to the Global Initiatives section of Chapter 4.

What we found

The investigation revealed that WhatsApp was violating Canadian and internationally accepted privacy principles, mainly in relation to the retention, safeguarding and disclosure of personal information.

- **Retention**

For WhatsApp to work, it needs to communicate with other mobile devices whose numbers are registered with WhatsApp. So we examined how a user's WhatsApp contacts list becomes populated with the mobile numbers of other WhatsApp users.

We found that the application retrieves this data from the address book on the user's mobile device. Once a user gives the application access to his or her address book, select information from the mobile device is periodically transmitted to WhatsApp to help identify other WhatsApp users.

This process, however, also retrieves the mobile numbers of people who are *not* subscribers to WhatsApp. Moreover, we discovered that WhatsApp retains those so-called "out-of-network" numbers. Although the numbers are stored in a protected form, the practice nevertheless contravenes an important privacy principle, which states that information should only be retained for as long as required for the fulfilment of an identified purpose.

- **Safeguards**

When the investigation began, messages travelling over the WhatsApp messenger service were unencrypted, leaving them vulnerable to

eavesdropping or interception, especially if they passed through unsecured Wi-Fi networks.

In September 2012, partially in response to our investigation, WhatsApp introduced encryption to its mobile messaging service.

Over the course of our investigation, we also noted that WhatsApp was generating passwords for message exchanges using information about the mobile device that is easily exposed. This created the risk that a third party could send and receive messages in the name of a user, without the user's knowledge.

Following our recommendations, WhatsApp strengthened its authentication process with a more secure system of randomly generated password keys. By the time our investigation ended, we noted that the security safeguards employed by WhatsApp appeared to be commensurate with the sensitivity of personal information at risk.

Nevertheless, we encouraged WhatsApp to remain vigilant when protecting personal information in light of a constantly changing threat environment.

- **Limiting Disclosure**

Another issue centred on the "status" updates that users choose to share with others. WhatsApp allows users to populate and share "user status submissions," which are tidbits of information limited to 139 characters. Typical status messages include "available," "busy," "at school," "at work," "sleeping," "in a meeting," and "urgent calls only."

Once a user's status has been inputted and saved, the status, which may contain personal information, is broadcast to all WhatsApp users who have the user's mobile number.

In our view, however, the potentially indiscriminate broadcast of status submissions was not within the reasonable expectations of users. Users could not adequately limit or control who received such messages.

Following our investigation, WhatsApp agreed to improve its notification to users, so that they understand that their status submissions will be widely broadcast. For instance, the organization committed to building real-time notifications, such as pop-ups, into future releases of the application.

Our Office does not have order-making powers. However, WhatsApp has expressed a willingness to comply with our recommendations in a timely manner. We will continue to monitor the company's progress in meeting commitments that it made in the course of our investigation.

Mobile Apps Guidance

The burgeoning popularity of smart phones, tablet computers and other mobile communications technologies has spawned a whole new world of mobile applications, or apps, such as reference tools and games.

Apps have become a rich part of our daily lives. They guide us to the nearest coffee shop, connect us with friends (and even complete strangers), entertain and amuse us, and swiftly settle arguments.

But they're not without risk. There's always the chance that someone will gain unauthorized access to your personal data, such as your address book or photos.

Some apps also come with device sensors that can track your whereabouts. In conjunction with data about your activities and preferences, it's possible to build a pretty precise portrait of you—without your knowledge and consent.

Consider, for example, how tricky it is for a software developer to convey privacy information to a person using an ordinary computer at a desk. Add to that the challenges of a small screen and the divided attentions of the average mobile user.

Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps (http://www.priv.gc.ca/information/pub/gd_app_201210_e.asp)

Compounding the difficulty is the lightning speed of the app development cycle: a fresh new app is begging to be downloaded long before you've had a moment to contemplate the privacy implications of the last one.

That's why our Office worked with our counterparts in Alberta and British Columbia to release a new guidance document for app developers last October. Entitled *Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps*, we wanted developers to understand that it is ultimately in their interest to embrace privacy protection. We are persuaded that mobile apps that take privacy seriously will be the ones that stand out from the competition and gain user trust and loyalty.

It's worth noting that a 2012 survey by the Washington, D.C.-based think tank, the Pew Research Center, revealed that 57 percent of app users in the United States have either uninstalled an app over concerns about having to share their personal information, or declined for similar reasons to install an app in the first place.

We focused on five important areas for app developers to consider, including a checklist to follow and further resources to ensure they have all the information necessary to build privacy into their designs.

2.8 COMPLAINT INVESTIGATION: *Telecoms company fails to adhere to its own policies on requests for access to personal information*

Background

A woman embroiled in a billing dispute with a telecommunications company after the cancellation of her Internet and wireless services account asked the company for all notes and transcripts of recorded conversations involving herself and the firm for the months of February and March 2010. She claimed the company did not respond to the request.

In July 2010, the woman was contacted by a collections agency. This prompted her to contact the telecommunications firms' chief privacy officer by registered mail, again requesting access to notes and transcripts of her recorded conversations.

An arrangement was ultimately reached between her and the telecommunications provider, and the final bill was paid.

The individual was then contacted by another collections agency, sparking a third request for access to her recorded interactions in February 2011.

The underlying dispute was resolved when the telecommunications company apologized for its actions, waived the account balance, and sought to remove certain remarks from her credit bureau report. The woman filed a complaint with our Office.

What we found

We confirmed that the telecoms company received the complainant's first access request in March 2010, as well as a later request.

However, the firm stated that, because it was in negotiations to settle the complainant's dispute over an extended period, its representatives mistakenly believed that it was not necessary to act on the request by giving the complainant the requested notes and transcripts.

The company affirmed that it has a policy of responding to requests for notes and transcripts of audio recordings within 30 days of receipt, free of charge. Audio recordings are typically retained for six months. If a recording is the subject of an access request, it is retained for an additional six months after a transcript is sent to the requester.

In this case, when the complainant made her third access request, the old audio recordings, transcripts of which were the subject of her earlier access request, had been purged. This was contrary to the firm's own internal policies and procedures.

The complainant was not given access to her personal information within the 30-day timeline set down by PIPEDA, nor was a 30-day extension communicated to or sought by the complainant. The firm was therefore deemed to have refused the access request.

What happened next?

In response to our preliminary report of investigation, the company amended its access-request policy and procedures to ensure consistency in their content.

It recognized and reaffirmed its obligations to respect the timelines set down by PIPEDA.

It also clarified its data-retention policy concerning personal information that is the subject of an access request and the need to set aside its normal destruction schedule for some time after a request has been served.

With regard to the training and education of staff, the firm's chief privacy officer issued a memo to

executives and managers reminding them of their privacy responsibilities and highlighted our concerns about the firm's actions.

He attached to the memo a copy of our *Accountability Guidelines*, as well as a presentation to executives and managers on the subject of account notes and audio recording requests.

The company also confirmed that these resources would be incorporated in orientation notes provided to all employees joining the department responsible for handling access requests.

Following the measures adopted by the firm, our Office concluded that the matter was ***well founded and resolved***.

Final thoughts

We encouraged the company to familiarize itself more thoroughly with our *Accountability Guidelines*. We especially highlighted the section on program controls, which state that an organization should adopt controls to ensure that what is mandated in its privacy governance structure is actually implemented in practice.

The guidelines also underscore the importance of adopting appropriate training and education programs. For example, employees who handle personal information directly require additional training that is tailored to their specific roles. Training also needs to be refreshed and the content updated to reflect changes.

Submission to CRTC Wireless Code Hearings

In October 2012 the Canadian Radio-television and Telecommunications Commission (CRTC) invited comments on its proposal to establish a mandatory code of conduct to govern the business practices of mobile wireless service providers.

Such a code is especially timely in light of the exploding popularity of smart phones and other mobile devices, and with many businesses embracing mobile payment systems.

Welcoming the opportunity to comment on the code, our Office delivered a submission to the CRTC. We expressed our support for the development of such a code, and urged that it be drafted to encompass an enterprise's obligations under PIPEDA.

Privacy compliance, we argued, is essential to the consumer trust and confidence on which the wireless economy depends.

2.9 COMPLAINT INVESTIGATION: *Summer camps trade information on child without parent's consent*

Background

A mother attempted to enrol her child in a particular summer camp for the first time. Let's call it Camp New. The woman submitted her application online and spoke with the director, who did not accept her child right away.

When her application was ultimately rejected, the woman filed complaints with our Office against both Camp New and another summer camp that her child had previously attended, which we will call Camp Old.

The mother was upset and believed that information about her child had been improperly shared between the two camps, possibly contributing to the decision by the director of Camp New not to accept her child.

Specifically, she alleged that Camp Old had disclosed her child's personal information to Camp New without her consent. At the same time, she alleged that Camp New had collected, used and disclosed her child's personal information to Camp Old without her consent.

What we found

Camp Old informed us that Camp New had, in fact, been in contact and had asked about the child and his previous camping experiences there. Camp Old admitted that, during their conversations, the two camps had exchanged information about the child. It added that this type of informal information exchange is normal practice among camping organizations.

The information shared included the child's recent application history and his past camping experience; an opinion about the child's personality; and an evaluation of the support the child required as a camper.

We were troubled to learn that Camp Old had no consent forms or policies regarding the disclosure of such information to third parties. We also found that privacy information on the organization's website was minimal and insufficient for obtaining consent.

For these reasons, we determined that Camp Old had not obtained the mother's consent to disclose her child's personal information to Camp New.

As for Camp New's application form (which the mother had authorized) and its privacy and confidentiality policies, none of these documents mentioned that the camp could collect camper personal information from other parties.

What's more, the language used in the camp's privacy documents was too vague for parents or guardians to understand the specific purposes for which personal information collected about campers would be used or disclosed.

As a result, we determined that Camp New had also failed to obtain the mother's consent for the collection, use and disclosure of her child's personal information.

What happened next?

Our Office issued a preliminary report of investigation to both camps. With such informal information exchanges said to be common practice among camps, we recommended that both camps obtain consent for any disclosure of personal information, and that they train their employees in their privacy obligations.

Both camps committed to implementing our recommendations within agreed-upon timelines. Consequently, we found the complaints to be ***well founded and conditionally resolved***.

2.10 COMPLAINT INVESTIGATION: *Store camera no longer captures neighbour's yard*

Background

After a retail store suffered a fire and several other security problems, the proprietor installed a video surveillance camera at the exterior back of the shop. In addition to the store's parking lot, the camera overlooked a public lane and some nearby homes and commercial properties.

The owner of the home directly behind the store complained to our Office about the camera. He alleged that, without his consent, it was capturing images of the back of his residence, his rear parking area, as well as any people going into or out of his home.

What we found

The storeowner told us that he needed the camera to guard against theft and vandalism. He detailed the security incidents that had occurred at the store in recent years and stated that a security guard was not affordable.

No notice was posted behind the store to alert people in the public lane that the camera was in operation. There were small stickers on the store's back door and on the camera, but these could not be read from a distance.

The camera's recordings were on a loop, so that images were overwritten every 72 hours. Recorded images were only archived in conjunction with suspected security incidents.

In light of the store's security history, we concluded that a security camera was an appropriate measure for videotaping the area around the rear of the store.

We did not, however, feel that capturing images of the neighbour's property constituted an appropriate purpose for the collection of personal information. By extension, those surveillance images should not be captured without the consent of the individuals concerned.

What happened next?

When we explained to the storeowner his neighbour's privacy concerns, he agreed to move the camera so that it would not capture images of the neighbour's home and parking area.

He also posted an appropriate notice at the rear door of the store, informing passersby that the public lane is under video surveillance and that their images will be recorded. The notice included contact information for the store.

We felt this was sufficient to establish the implied knowledge and consent of people approaching that area. Even so, we encouraged the storeowner to try to minimize any unnecessary surveillance of the public lane.

We concluded the complaint was ***well founded and resolved***.

When the storeowner told us he still wished to reserve the right to move the camera to the original position should circumstances dictate, we cautioned him against once again capturing images of the back entrance of the complainant's home and his parking area, on the grounds that this would violate PIPEDA. We strongly urged him to read and follow our *Guidelines for Overt Video Surveillance in the Private Sector*.

2.11 DATA BREACHES

Accountability obliges organizations that experience a data breach to take whatever steps they can to minimize the impact of the breach. That means rapid and comprehensive intervention to stop the damage, alert authorities, and assist and communicate with the individuals affected.

When the immediate emergency has passed, it also means scrutinizing internal policies and processes, and taking all necessary steps to strengthen them against future incidents.

Our Office encourages organizations to voluntarily report data breaches that involve personal information. These breaches fall into three broad types:

Accidental disclosure involves incidents where an organization discloses personal information to unintended recipients by accident. For example, bank statements may be sent to the wrong address through mechanical or human error, or personal information is made publicly available on an organization's website through a technical glitch.

Loss refers to incidents where personal information in the hands of an organization goes missing, usually through the loss of a laptop, CD or paper documents.

Unauthorized access, use or disclosure encompasses any incident in which personal information is accessed, used or disclosed by someone without an organization's authorization. Examples include the

theft of a laptop, an online hack of an organization's database, or an employee accessing or using personal information for unauthorized purposes.

In 2012, 33 private-sector data breach incidents were voluntarily reported to us. This is a decrease of nearly 50 percent from the 64 incidents reported to us the year before, and represents the lowest number of breaches reported to us in the past five years.

Sector	Accidental disclosure	Loss	Unauthorized access, use or disclosure	Total	Proportion of breaches by sector
Financial	4	2	13	19	58%
Services			1	1	3%
Insurance	2			2	6%
Sales/Retail					
Telecommunications			3	3	9%
Internet			1	1	3%
Entertainment	1		2	3	9%
Accommodations	1		1	2	6%
Other		1		1	3%
Health					
Professionals	1			1	3%
Transportation					
Total	9	3	21	33	
Proportion of breaches by type	27%	9%	64%	100%	100%

The financial industry is always the leading sector in routinely reporting breaches to us. Last year, it reported 19 breaches, down 34 percent from the 29 reported the year before.

Breach notifications from all other sectors totalled 14, dropping back from a high of 35 in 2011 to levels comparable to other years.

The volume of voluntary breach notifications that reach our Office is obviously affected by the number of breaches that actually occur. However, other factors are also at play, including the level of awareness among organizations about our Office's role in receiving such notifications and the choices organizations make about whether to report incidents when they occur.

In light of this variability and the relatively small numbers involved, we cannot explain the reduction in breach notifications in 2012, relative to the year before. However, we will continue to monitor the numbers to search for meaningful trends.

For their part, private-sector privacy officers continue to maintain that they are proactively reporting breaches, even though federal legislation to make notifications mandatory has not been passed into law. We commend them for continuing to do so on a voluntary basis.

When we receive a breach report our Office works with the organization's privacy officer to ensure that the necessary steps are taken to mitigate any fallout. In cases that warrant notification to individuals, we want to ensure that affected individuals are provided with consistent information, and that their concerns are addressed in the best and fastest possible manner.

We believe it is in everybody's interest to curb potential problems before they escalate into formal complaints to our Office. Here are some examples of breach incidents reported to our Office in 2012:

2.11.1 *LinkedIn moves quickly to stem damage from major cyber-attack*

In June 2012 LinkedIn, a business networking site, had nearly 6.5 million user passwords stolen and posted online. While the breach exposed certain weaknesses in its information safeguards, LinkedIn was swift in its breach response and co-operative with our Office and our counterparts in British Columbia, Alberta and Quebec.

Its commitment to remediation clearly flowed from the top, with senior management authorizing a "Code Red" response that rendered the breach the top priority for the organization and triggered an immediate deployment of resources to deal with the breach.

Afterwards, LinkedIn followed up by reviewing their response, assessing what they learned, and further strengthening their information security measures.

LinkedIn, like many organizations, could have had better safeguards for information to begin with. But when we looked at the company's breach response in the face of a cyber-attack, we found the organization had demonstrated due diligence and accountability.

2.11.2 *Investor services employee responds to phishing e-mail*

An employee of a financial investment services company responded to a "phishing" e-mail that appeared to originate from a large bank. The fraudulent e-mail requested the confirmation of a user ID and password. The information was then used to access corporate accounts and view the banking information of a small number of clients.

The investment services company immediately deactivated the compromised user ID and password and notified local police, the RCMP's fraud unit and our Office.

Affected clients were notified of the breach and advised to monitor their account activity. As an added precaution, they were also advised to contact the two major credit bureaus to place a fraud alert on their files.

2.11.3 *PASSWORD INFORMATION STOLEN WITH LAPTOP COMPUTER*

A financial adviser working as an independent contractor for a financial services company had a laptop computer, USB key and day planner stolen from a locked car. The stolen material included sensitive identity and financial information of 188 clients.

The computer was password protected with encryption, but the password and encryption software were noted in the day planner.

The company notified local police as well as our Office. All affected clients were contacted and offered free credit-monitoring services.

2.12 UPDATE ON GOOGLE'S PRIVACY POLICY: *Concerns about linking and retaining data remain*

In March of last year Google introduced a new privacy policy. As the company had acquired numerous other enterprises and services, each with its own set of privacy policies, Google decided to integrate them into a single policy that would be short and simpler to read.

The integration was also intended to reflect Google's efforts to streamline its services for Google account holders. This meant that if a Google account holder is signed in, Google would combine information that the account holder had provided from one service with information from other services.

From Google's perspective, this would mean a "simpler, more intuitive Google experience." By combining data in this way, Google also proposed to improve search results and make ads more relevant to individual users.

We examined the privacy implications of the changes in Google's policy, focusing in particular on a lack of specific information relating to data retention, the implications of linking personal information of account holders across services, and the implications for users of mobile devices running Google's Android operating system.

We asked Google to include more information about its data retention practices in its privacy policy and to more fully inform account holders about the linking of their personal information, and how they can choose to prevent this.

We were not the only data protection authority to express concerns to Google. The Asia Pacific Privacy Authorities (a group in which we are active), as well as the Article 29 Working Party, led by the *Commission nationale de l'informatique et des libertés* (CNIL), also wrote to Google, urging it to make certain revisions. The CNIL/Article 29 Working Party had conducted a very thorough review of the new policy and made specific recommendations to the company.

As of the writing of this report, Google has not changed its privacy policy, or indicated whether it would do so.

2.13 COMPLIANCE AUDIT UPDATE: *Independent authority confirms Staples addressed privacy concerns*

In June 2011 our Office published the report of a compliance audit that we conducted into the personal information management practices of Staples Business Depot.

The audit was prompted by prior investigations into complaints about electronic devices that had been bought, used, returned to the store and then resold, with the personal information of the original buyer still residing on them. Our Office confirmed that a range of data-storage devices were being resold without all of the residual data being fully erased, resulting in the improper disclosure of personal information.

The comprehensive audit we subsequently conducted resulted in 10 recommendations, which Staples agreed to address. Among our recommendations, we encouraged Staples to:

- review procedures and processes for wiping electronic data-storage devices and implement enhanced controls to eliminate the risk of personal information being disclosed;
- limit the retention of personal information accompanying online orders for printing or copying;
- ensure that personal information is stored in locked cabinets or secured areas;
- develop privacy-specific compliance reviews as part of its internal audit program; and
- assign employees unique system-access credentials.

When the audit was published, the Commissioner requested that Staples hire an independent firm to verify that it had implemented all actions in response to the recommendations.

What happened next?

Staples hired an independent firm, which verified that Staples had taken action to address our recommendations, and that new procedures were in place. In particular, the independent audit confirmed that Staples had implemented a process to eliminate customer data from returned products.

The audit firm said it was satisfied that the new procedure would ensure that all customer data from a data storage device would be deleted prior to being resold.

Responding to Your Privacy Preoccupations

In 2012, we continued our efforts to assist Canadians who were puzzled about new information technologies, concerned about their rights under the privacy law, or angered by the way private enterprises treat their personal information.

The privacy-related preoccupations of Canadians prompted thousands of requests for information, and hundreds of complaints to our Office. As always, we made every effort to respond to their concerns with care and respect, and to deliver solutions that were appropriate and timely.

This chapter outlines the work in 2012 of our Information Centre and our investigative teams on matters related to PIPEDA. It highlights our ongoing efforts to streamline and improve our processes, for the benefit of complainants and respondents alike.

Our Office also dedicated itself to the advancement of privacy-related knowledge. This chapter highlights our research-funding Contributions Program, which was refurbished in 2012 with a new five-year strategic plan, as well as other work we conducted or commissioned in areas as diverse as web leakage, predictive analytics, and online direct-to-consumer genetic testing.

We also summarize here key insights we gleaned from business through our biennial survey of the privacy attitudes and practices of Canadian enterprises. Indeed, engaging with stakeholders is a priority for us, so this chapter also reviews the broad range of outreach efforts undertaken by our Office, both in Ottawa and through our Toronto presence.

The knowledge we generate through these many avenues informs our work in a multitude of ways. Among other things, it ensures that the guidance, policies and other tools we create are factual, up-to-date, and relevant to the needs of the target audience. In addition to the new accountability guidance described in Chapter 2, other documents we published in 2012 explored such specialized topics as cloud computing, online behavioural advertising and mobile applications.

As this chapter explains, our goal is to bolster voluntary compliance with PIPEDA among organizations. Over time, we hope that translates into fewer privacy problems for Canadians.

3.1 INFORMATION CENTRE

Our Information Centre received 4,474 requests for information about private-sector privacy issues in 2012. About nine in 10 requests for information were made by phone, as in past years.

The telecommunications sector accounted for 14 percent of the information requests, representing the single largest category. This was followed closely by the banking sector (13.5 percent of all information requests). We also received a significant number of requests for information related to the rental accommodation sector, representing five percent of our total request load.

In terms of the substance of their inquiries, Canadians were mostly concerned about the possible disclosure of personal information without their consent, and how their identities and personal information are handled by organizations. Calls increased whenever there was a well-publicized data breach.

As in every other year, our Office continued to receive many calls about the collection of sensitive forms of personal information, notably the Social Insurance Number. Callers also sought information on how to gain access to their personal information in the hands of enterprises.

And we received numerous requests for details about our Office's privacy complaints process.

3.2 COMPLAINT INTAKE

Our PIPEDA Investigations branch continued in 2012 to focus on finding effective resolutions to the privacy concerns of Canadians.

And so, over the summer, we made it easier for Canadians to reach us through their fingertips, in order to help them more efficiently assert their privacy rights. We introduced an online complaint form that allows Canadians to describe their concerns, attach supporting documents, and submit their complaints through our secure online portal, thus eliminating the need to print, mail or fax us the documents.

We also sought to close more cases in a timely manner, and in a fashion satisfactory to both complainants and respondent organizations. Delays are not satisfactory for anyone, and can saddle us with a burdensome backlog of cases.

Toward that end we continued to ensure that we were optimizing our choice of channels through

which to deal with complaints. Our Intake Unit played a key role in assigning cases appropriately, whether that was to our Early Resolution Officers, to our formal investigative process, or to other bodies more appropriately suited to deal with the underlying dispute.

We also pursued negotiations that would lead to a settlement of the issues and, under certain circumstances, we used the Commissioner's discretionary powers to decline or discontinue investigations.

Overall, we sought to keep our eye on the significant issues—the complaints that raise serious and broad systemic issues posing the greatest privacy risks for Canadians.

One gratifying outcome of these initiatives is that the 145 formal investigations we completed in 2012 marked a 21-percent increase from the year before.

3.2.1 *Written Submissions Received*

All written submissions about privacy matters, excluding only those against federal government institutions, are forwarded to the PIPEDA Intake Unit for initial triage. In 2012 we received 705 such written complaints, in line with the numbers we received in other recent years.

The Unit reviews the submission and, where necessary, follows up with the complainant to clarify our understanding and to gather any other necessary information or documents.

If the complainant has not already discussed the problem with the person responsible for privacy within the relevant organization, an officer in the Intake Unit will ask the complainant to try to resolve the issue with the organization directly, and to re-engage our Office if that proves unsuccessful.

About one-quarter of these complainants were redirected to the privacy officer of the organizations in question, in an effort to resolve the issue quickly and directly.

Our Intake officers are often able to resolve issues immediately, eliminating the need for a formal complaint.

For instance, we might advise a complainant that a previous investigation revealed that the activities being complained about are actually permitted under PIPEDA. Similarly, if we have previously determined that we don't have jurisdiction over the organization or type of activity, our officers will try to redirect the individual to other resources or assistance.

Another one-third of the complaints were not accepted on the grounds that there is no indication of a contravention of PIPEDA, or that we do not have jurisdiction. Others were not accepted for further treatment because there was insufficient information to investigate, or the issue was resolved satisfactorily during the Intake process.

3.2.2 *Complaints Accepted by Industry Sector*

In the end we accepted 220 complaints in 2012, which were then channelled either through our Early Resolution process or into our more formal investigations process.

About one in four of these complaints related to the financial sector, which includes banks, credit card companies, loan brokers, financial advisers and related enterprises. This trend is observed every year, most likely because of the size and scope of the sector and the huge number of sensitive transactions it handles.

Our experience is that financial institutions develop some of the most robust privacy policies and practices in the private sector. And yet there is room for improvement, particularly in the consistent application of policies and practices related to collection, employee training, and safeguarding of personal information.

The telecommunications and Internet services sectors were the two categories with the next-highest number of complaints—about half each as many as were accepted in the financial sector. This trend reflects the growing prominence of the digital economy, along with the privacy risks inherent in the use and exchange of so much personal information.

The majority of telecommunications-related complaints dealt with access to account information. Those related to the Internet were more diverse, including issues of consent and the use of posted information.

Industry sector with most complaints, as a percentage of all complaints accepted*

Sector	2012	2011	2010
Financial	22	22	22
Telecommunications	11	11	9
Internet Services	11	6	9
Services	10	10	17
Insurance	7	9	13

* Statistics and definitions for all industry sectors can be found in Appendix 2

3.2.3 *Types of Complaints Accepted*

The top-three types of complaints we accepted under PIPEDA last year related to:

- problems in gaining access to personal information
- the inappropriate use and disclosure of personal information and
- the over-collection of personal information.

This was similar to other years, except that access queries overtook complaints about the use and disclosure of personal information as the chief issue of concern.

Access complaints can centre on the full or partial denial of access to personal information; undue delays in receiving requested information; or disagreements over the definition of what constitutes personal information that a business is obliged under PIPEDA to provide.

Most common categories of complaints, as a percentage of all complaints accepted

	2012	2011	2010
Access: Complaints about difficulties gaining access to personal information.	30	26	24
Use and disclosure: Complaints involving allegations that personal information was inappropriately used or disclosed, without consent, for purposes other than those for which it was collected.	26	32	27
Collection: Complaints involving the unnecessary collection of personal information or personal information collected unfairly or unlawfully, such as without proper consent.	15	20	16

3.3 EARLY RESOLUTION OF COMPLAINTS

When we accept a written complaint that appears amenable to a speedy resolution, the Intake Unit refers the case to an Early Resolution Officer. The officer works with the complainant and the respondent organization to resolve the complaint in a co-operative and often conciliatory manner.

Issues that can take months to resolve through the formal complaint investigation process can be concluded in days through our Early Resolution process. The process has been applauded in recent years by both complainants and respondent organizations.

In 2012, we attempted early resolution with 138 complaints, up 10 percent from the year before. We were able to reach a satisfactory conclusion in 115 of these cases, or 83 percent. The remaining 23 cases were reassigned for formal investigation.[2]

Cases accepted for early resolution	Cases resolved through early resolution	Cases referred for further investigation
138	115	23

On average, complaints handled in this manner were closed in 2.8 months from the date of acceptance. While this was up slightly from the average treatment time of 2.0 months the year before, early resolution remains a significantly speedier option than formal investigation.

Here are some examples of cases that were successfully closed through our Early Resolution initiative.

3.3.1 *Utility company curbs collection of personal data*

A person who applied online for services from a utility company was concerned about mandatory fields requiring applicants to provide their Social Insurance Numbers, driver's licence numbers, and information about their employers.

When asked, the company said the information was required to authenticate customers contacting the company. The individual was not satisfied with the response and filed a complaint with our Office.

The Early Resolution Officer contacted the company and informed it about the limited range of circumstances under which Social Insurance Numbers and driver's licence numbers may be collected, and on the dangers of over-collecting information in about employers. The Officer also furnished the utility company with several of our guidance documents.

In response, the utility stopped collecting driver's licence numbers and Social Insurance Numbers, and no longer makes employer information mandatory. It replaced this information with security questions designed to authenticate the identities of account holders.

The company appreciated the information we provided and the complainant was satisfied with the company's actions.

3.3.2 *Foreign retailer swaps SIN for PIN*

A customer of a direct-marketing retail company was required to provide her Social Insurance Number in order to receive a discount on a purchase. When challenged, the company explained that it uses the last four digits of the number to authenticate its "preferred customers".

[2] Detailed statistics on the sector, type and dispositions of early resolution interventions may be found in Appendix 2

Before complaining to our Office, the customer read the guidelines on our website for the appropriate use of the Social Insurance Number, and contacted our Information Centre to see if she had a valid complaint under PIPEDA.

Our Early Resolution Officer contacted the company, which was based outside Canada, to advise it that requiring customers to provide Social Insurance Numbers in this context, and using them as identifiers were not reasonable practices under PIPEDA.

The Officer highlighted the sensitivity of the number, and how collecting it posed a potential liability for the company in the event of a data breach.

In response, the company pledged to retrain its call centre and sales staff so that they would no longer request Social Insurance Numbers. Instead, customers would be asked to select a four-digit Personal Identification Number, or PIN.

The organization also said it would change its forms to remove references to Social Insurance Numbers (or the equivalent in other countries).

The company reacted swiftly and made significant changes to conform with PIPEDA. The complainant was satisfied with these actions.

3.3.3 *Insurance firm purges old records to comply with retention rules*

An individual contacted an insurance company to obtain a quote for a policy. He learned that the company still had a record of a quote it had provided to him five years earlier.

The individual, who was not a customer of that insurance company, objected to the organization retaining his information and requested that his original quote be deleted. The company declined.

After the individual complained to our Office, our Early Resolution Officer advised the insurance company that personal information may only be retained for as long as necessary to fulfill the purposes for which consent was originally obtained from the individual.

In response, the firm launched an extensive program to correct the excessive retention of personal information, including initial policy quotes, in its databases and to bring its practices in line with PIPEDA.

The complainant was satisfied with the response.

3.3.4 *Company retrains staff to handle privacy queries*

A customer who had some concerns about the privacy practices of a subcontractor of a large retailer had difficulty finding the appropriate avenue to raise his concerns.

The employees he spoke with were unfamiliar with the company's privacy obligations under PIPEDA, and were unable to direct him to their privacy officer, as required under the accountability principle in PIPEDA.

When contacted by our Early Resolution Officer, the company was surprised to learn that, despite trying several avenues, the customer was never directed to the individual appropriately charged with privacy matters.

The company promised to implement a mandatory staff training course to improve the capacity of employees to deal with privacy complaints, including directing people to the appropriate authorities.

The complainant was satisfied with this commitment.

3.4 SERVING CANADIANS THROUGH COMPLAINT INVESTIGATIONS

Not all complaints are good candidates for early resolution. Complaints that raise complex, new or potentially systemic issues will continue to be addressed through our formal investigation process.

In 2012 we completed 145 investigations of complaints under PIPEDA, 21 percent more than the year before. In the vast majority of the cases (140 of the 145), we were able to find a satisfactory conclusion to the issues. Only five investigations resulted in complaints being deemed "well founded," which means there was no resolution that we found acceptable.

Investigations completed	Investigations concluded with satisfactory outcome	Complaint deemed well founded; case remains unresolved
145	140	5

Despite the significant hike in the number of complaints we accepted for formal investigation, the average time to complete such investigations dropped to 12.6 months in 2012, down 12 percent from 14.3 months the year before.

When combined with early resolution complaints, the overall average time to close a file was 8.3 months in 2012, nearly identical to the year before and well within the 12-month requirement set out in PIPEDA.

We were pleased to note that, even as we investigated more cases, and saw some improvements in our treatment times, we were at the same time able to reduce the size of our outstanding case list. By the end of the year, we had 141 active complaints still under review, a 20-per-cent drop from the 177 cases that remained active at the end of 2011.

These encouraging trends are at least partly due to the continuing success of our early resolution efforts. Of the total of 260 complaints we handled in 2012, 115, or 44 percent, were closed through early resolution strategies.

Further statistics on the sector, type, and dispositions of completed investigations can be found in Appendix 2. Summaries of numerous cases we investigated may be found in Chapters 1 and 2.

3.5 ADVANCING KNOWLEDGE

3.5.1 *Contributions Program*

In 2012 we issued our 10th annual call for proposals under our Office's Contributions Program, regarded as one of the foremost existing privacy research programs. We also developed a new six-point strategy to further increase the impact of the program on the Canadian privacy landscape.

Here are some of the projects we funded in 2012:

- A study of the privacy challenges emerging from innovations in cell therapy research;
- An analysis of the scope of voluntary information sharing by private enterprises to law enforcement for investigations into cybercrime;
- The development of a series of in-depth news reports and other informational tools for francophone radio and web sites that provide practical information about protecting personal information;
- An interactive mapping tool to help Canadians better understand cloud computing and its impact on their personal information;
- An investigation of smartphone applications and the risks to end-user privacy; and
- A report on the privacy implications of using information technology in situations involving domestic violence, sexual violence and stalking.

The program, which is mandated under PIPEDA, funds independent privacy research and related knowledge-translation initiatives.

The Contributions Program encourages researchers to propose projects that generate new ideas and knowledge about privacy and that can translate those ideas into improved personal information management practices among organizations and more informed decision-making by Canadians.

A call for proposals takes place in the fall of every year. Academic institutions and not-for-profit organizations are eligible for funding. Projects are selected through a competitive process and the resulting research effort is carried out in a manner independent of our Office.

Since its inception under PIPEDA and subsequent launch in 2004, the program had allocated approximately $3 million to nearly 90 initiatives. The program's budget is $500,000 per year, and the maximum that can be awarded for any single project is $50,000.

New strategy

In order to further increase the program's impact among our stakeholders and in Canada generally, we adopted a new five-year strategy in 2012. The strategy is founded on six points:

- **Leveraging impact through partnerships**
  We explored partnership opportunities with other federal funding agencies. As a first step, we engaged the Social Sciences and Humanities Research Council and Industry Canada as collaborators in the organization of a *Pathways to Privacy Research Symposium*. (Please see sidebar for more information.)

- **Enabling knowledge translation and application**
  We revised our Call for Proposals in order to encourage research applicants to integrate knowledge-translation plans into their projects. The objective is to facilitate the adoption of research results by end users. The *Pathways to Privacy Research Symposium* series and some related material to be published in 2013 aim to showcase the real impact that our funded projects are having on the lives of Canadians.

- **Strengthening peer review**
  For the first time in 2012, we created a college of external peer reviewers whose members come from academia, civil society and government, with a view to broadening the range of expertise in the program's evaluation process. External peer reviewers complement our own internal perspectives and serve as excellent ambassadors for the program.

- **Facilitating access through technical enhancements**
  We renovated the Contributions Program section of our Office's website, making funded projects more easily searchable and accessible to end users and relevant stakeholders.

- **Evaluating the success of the program**
  We conducted a bibliometric study of the program's deliverables over the years, to evaluate the extent to which the research was taken up by the community in academic journals, articles, websites, and on social media.

- **Renewing our public communications strategy**
  A new, proactive communications strategy was developed and is being implemented, with a view to better promoting the funding opportunities available under the Program and showcasing the real outcomes of funded projects. Better communication will also help potential applicants learn about the program's existence, so that we can continue to attract top-quality research proposals.

Research Symposium and In-house Learning

On May 2, 2012 our Office hosted our inaugural *Pathways to Privacy Research Symposium* in Ottawa. The symposium series is intended to showcase privacy-related research funded by our Contributions Program and partner organizations. It also aims to promote dialogue between the researchers and the people whose lives and businesses are being affected by the resultant knowledge.

The theme of the first symposium was *"Privacy for Everyone,"* and the topics included the changing privacy landscape for youth, reaching diverse populations, cultural perspectives on privacy, and frontiers of identification and surveillance among different populations.

More than 130 participants from academia, government, non-profit organizations and privacy regulators attended the daylong event, organized with the assistance of the Social Sciences and Humanities Research Council of Canada and Industry Canada.

Meantime, our Office also developed an in-house speaker series, dubbed *Privacy Conversations*, to promote dialogue and knowledge exchange across our own organization.

We were treated to an overview of recent privacy-related jurisprudence, as well as presentations on predictive analytics, mobile applications and the latest results of research funded under our Contributions Program.

3.5.2 *Research on Web Leakage*

"Web leakage" involves the disclosure of a website user's personal information to third-party sites without the user's proper knowledge or consent. Websites that do not take care to limit disclosure can leak a wide range of personal information, such as names, e-mail addresses and other data, to third parties.

Since web leakage is becoming a growing concern internationally[3], our Office in 2012 undertook some research to determine whether Canadian websites were also leaking the personal information of users to third parties. We posted our findings in September, showing that several sites popular among Canadians did, indeed, leak personal data, in some instances to a significant degree.

The technology backstory

When a person visits a website belonging to a specific organization, the content on that site might come from different sources outside of the organization. For example, a website may obtain revenue by allowing third-party organizations to place advertisements on its site, or contract certain functionality out to third-party service providers.

In the case of a third-party advertisement, when a user loads a page on a participating website, the website operator sends a request to an advertiser,

[3] http://w2spconf.com/2011/papers/privacyVsProtection.pdf

requesting that an ad be placed on the web page. In the process of making such an "ad call," the website may disclose personal information about the user to a third party, such as the advertiser.

In addition, websites may set a cookie in a user's browser, and that cookie can contain personal information. If the cookie is shared with a third party, there could be a disclosure of the personal information contained in the cookie.

These forms of online disclosure to third parties, through methods such as web requests, cookies and others not discussed here, have been referred to as "web leakage."

Our research

In July and August 2012 we tested 25 sites popular with Canadians. Most of the sites were subject to PIPEDA, but the research also included a couple of the sites operated by organizations subject to the *Privacy Act*.

We created some test accounts from which we submitted personal data such as fictitious contact information. We then checked to see whether some or all of this data was finding its way to third parties.

We identified significant privacy concerns with six websites, and had some lesser issues with a further five. These sites appeared to be leaking some of the personal information submitted by users when signing up for an account on a particular site. The other 14 sites we tested did not appear to be leaking personal information.

According to our analysis, the third-party organizations that obtained our personal information fell into three main categories:

- Advertising companies, which are responsible for supplying third-party ads for websites;
- Analytics companies, which measure, collect, analyse and report website usage data for purposes such as marketing and improving aspects of a website; and
- Electronic flyer (e-flyer) services, which provide such services as weekly flyers to websites that feature special promotions, often tailored to a specific region.

What happened next?

The Privacy Commissioner sent letters to the 11 organizations whose websites we had found were leaking personal information. She asked them to provide information about their practices and, where appropriate, to explain how they will change their practices to comply with the privacy law.

The Commissioner was reassured by the careful attention that almost all of the contacted organizations gave to this matter. She saw a number of positive changes as a result of this research, and felt that it provided a good first step toward ensuring that Canadian websites obtain meaningful consent for the collection, use and disclosure of users' personal information.

Stakeholder outreach also followed this research. Our Office met with industry associations and individual stakeholders working towards a common goal of better privacy compliance.

This concrete exercise underscored that organizations need to better adapt their privacy policies and consent processes to meet today's online reality. Along with our provincial counterparts, our Office will be setting out guidance for obtaining meaningful consent online.

3.5.3 *Understanding Predictive Analytics*

The data bits that people inadvertently leave behind by their Internet browsing, social media interactions, use of retail loyalty cards, and many other commonplace activities have become glittering gold for companies looking for ways to target their marketing efforts.

Indeed, in a shiny new trend called predictive analytics, people's data trails can be mined for clues about their personal habits, preferences and shopping intentions.

More broadly, predictive analytics is a branch of data mining that is concerned with forecasting probabilities. Indeed, it is a general-purpose analytical process that can be applied in sectors as diverse as retail to boost sales, law enforcement to predict crime, and health programs to monitor for disease outbreaks.

News that an American department store giant used predictive analytics to assess which women were likely to be in their early stages of pregnancy, and thus more amenable to ads for baby items, helped illuminate the phenomenon.

Analytics tools such as this pregnancy-prediction algorithm function behind the scenes, making it difficult, if not impossible, for people to know how their personal information is being used.

What's more, these practices are becoming increasingly prevalent and potentially intrusive.

For these reasons, our Office decided to explore the practice in our in-house research program, and to produce a report for publication in the coming year. It's part of an ongoing effort to understand the value "of Big Data" to organizations, and to reflect on the privacy implications of such emerging technologies.

3.5.4 *Online Direct-to-Consumer Genetic Testing*

Advances in medical science and information technologies have made genetic testing more accessible and affordable. People can now obtain kits from online genetic testing companies to find out whether they are at heightened risk of developing certain common medical conditions, without ever having to consult a doctor.

But as such direct-to-consumer genetic testing becomes more popular among individuals, insurance companies are also spotting an opportunity. If genetic testing can peer into a person's future, then insurers are naturally keen to weave this information into their risk assessments.

There are no laws in Canada that specifically address the use of genetic test results for non-medical uses such as assessing risk for insurance purposes. However, under PIPEDA, any collection of personal information for a commercial purpose must satisfy the "Limiting Collection" Principle of the Act. The law further specifies that an organization "may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."

To help us understand and assess this rapidly evolving field, which we identified some years ago as one of our four policy priorities, our Office commissioned two papers from academic experts. The papers, available on our website, were prepared by Prof. Angus Macdonald, of the Department of Actuarial Mathematics and Statistics and the Maxwell Institute for Mathematical Sciences at Heriot-Watt University in Edinburgh, as well as by Prof. Michael Hoy, of the Department of Economics and Finance at the University of Guelph, Ont., and Maureen Durnin, an independent researcher, also of Guelph.

We also asked Dr. Steve Scherer, Director of the Centre for Applied Genomics at Toronto's Hospital for Sick Children, to respond to a set of questions on the predictive value of genetic information. These have also been posted on our website.

To further refine our thinking on the issue, we invited experts to a roundtable to discuss the commissioned research papers and the Canadian Life and Health Insurance Association's position on the use of genetic test results.

3.6 ENGAGING WITH BUSINESS

A vital part of our mandate is to engage with stakeholders—to listen to their concerns and to share what we know about privacy. In 2012, individuals within our Office delivered 101 speeches at events such as the Digital Commerce and Internet Law Forum; the Canadian Business Communications Conference; the national launch of the Canadian Identity Theft Support Centre; the Canadian Bar Association's *Privacy and Access Symposium*; and the International Association of Business Communicators' *Canadian Business Communicators Conference*.

3.6.1 *The Toronto Office*

Our Toronto Office is building a strong presence in the Greater Toronto Area for core activities of the Office of the Privacy Commissioner of Canada.

We located a branch of our Ottawa Office in Toronto because many industry associations and organizations are headquartered there, along with many PIPEDA stakeholders. Since then, the vision of the Toronto office has expanded to encompass collaboration with a range of stakeholders, with a view to improving industry compliance with PIPEDA and, as a result, benefiting Canadians.

By listening to stakeholders, our Office is better able to understand the issues and priorities of business. Such meaningful engagement also furnishes us with the context necessary to ensure that the guidance and communications materials we provide are timely and relevant.

A key aim of our outreach is to encourage more voluntary compliance with the private-sector privacy law, thus leading to fewer complaint investigations. The continued dialogue and exchange of information will also build more awareness and privacy protections for Canadians.

3.6.2 *Business Survey*

In early 2012 we published another comprehensive survey of businesses, which found that Canadian companies are storing ever more personal information digitally, but that many are not applying the tools or practices necessary to protect this data.

The *2012 Public Opinion Survey on Canadian Business and Privacy-Related Issues* was a follow-up to polls we completed in 2007 and 2010. The surveys help us understand how private-sector organizations are thinking about and responding to privacy challenges.

2012 Public Opinion Survey on Canadian Business and Privacy-Related Issues (http://www.priv.gc.ca/information/por-rop/2012/por_2012_01_e.pdf)

At our outreach events, one of the things that businesses told us they most wanted was a handy list of privacy pitfalls and how to avoid them. In reviewing the complaints we received under PIPEDA in recent years, we developed this list of top-10 tips to help organizations avoid the most commonly reported privacy problems:

1) Post contact information for your privacy officer on your website.
2) Train staff about privacy.
3) Take responsibility for employee actions.
4) Limit the collection of personal information.
5) Make the use of Social Insurance Numbers as identifiers optional.
6) Driver's licences: You can look at them, but don't record them.
7) Tell customers about video surveillance.
8) Protect personal information.
9) Respond to requests for access to personal information.
10) Be upfront about your collection and use of personal information.

The telephone survey of 1,006 companies of various sizes and sectors across Canada found that organizations are storing personal information on a variety of digital devices, such as desktop computers (55 percent), servers (47 percent) and portable devices (23 percent).

Nearly three-quarters of them (73 percent) are using technological tools such as passwords, encryption or firewalls to prevent unauthorized access to the personal information stored on these devices.

However, the poll also suggested that many businesses may not be making the most of the safeguards available for these technologies.

For example, passwords are the most popular technological tool that businesses use to protect personal information, accounting for 96 percent of all measures used. However, nearly four in 10 businesses using passwords lack controls to ensure that those passwords are difficult to guess, and 27 percent never require employees to change passwords.

The survey also found that nearly one-quarter of businesses store personal information on portable devices, such as laptops, USB sticks or tablets, which are more vulnerable to theft and loss than desktop computers. Nearly half (48 percent) of companies who use such portable devices said they don't protect the information with encryption.

In terms of attitudes toward privacy, the poll turned up mixed results.

For example, while three-quarters (77 percent) of respondent companies said privacy protection is important, only six in 10 (62 percent) have a privacy policy, half (48 percent) have procedures to deal with customer complaints about the handling of their personal information, and one-third (32 percent) have staff trained in privacy laws and practices.

On the plus side, the majority (57 percent) of companies that have a privacy policy update it at least once a year, and nearly four in 10 (39 percent) view the protection of privacy as a competitive advantage.

3.7 GUIDANCE, POLICIES AND TOOLS

Our Office conducts or commissions research, we talk and engage with provinces, we collaborate internationally, and we engage with the private sector, both through our main Ottawa Office and our Toronto office. All this feeds into our development of guidelines, interpretation bulletins, policy statements, fact sheets and other tools.

This section describes key guidance and other tools we disseminated in 2012. They are in addition to these three publications, described elsewhere in this report:

- *Getting Accountability Right with a Privacy Management Program*, produced in association with our counterparts in Alberta and British Columbia. The document and an associated interpretation bulletin set out our expectations for privacy programs and the need for organizational commitments and program controls. For more detail, please see section 2.1 of this report.
- *Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps* was released by our Office in October 2012. It aims to persuade developers of mobile applications that privacy protections benefit users and build trust in the product. The guidance is described more fully in a sidebar in section 2.7 of this report.
- Our Top-10 Tips for avoiding the most common privacy pratfalls are described in section 3.6.1, above.

We believe that listening to stakeholders ensures that our guidance products are relevant, timely and useful. That, in turn, boosts the likelihood of compliance and decreases the probability of complaints—a clear benefit to companies, Canadians, and us.

3.7.1 *Policy on Online Behavioural Advertising*

Online behavioural advertising is a practice in which people's web browsing activities are tracked across websites and over time, so that their interests can be inferred and tailored ads targeted to them. The business interests involved in such online tracking, profiling and targeting (collectively referred to as online behavioural advertising), include the advertising industry, browser developers and website operators.

The practice uses such technologies as web cookies, web beacons, supercookies, zombie cookies and device data to collect and use information about an individual's web-based activities. Our Office takes the view that the collected data includes personal information that falls under the application of PIPEDA.

Toward that end we released in December 2011 a set of *Online Behavioural Advertising Guidelines* to govern the appropriate collection and use of data in the course of this practice. Then, to further explain the underlying rationale behind our guidelines, we followed up in 2012 with a policy.

Policy Position on Online Behavioural Advertising (http://www.priv.gc.ca/information/guide/2012/bg_ba_1206_e.asp)

Among other things, the policy urges businesses engaged in online behavioural advertising not to track the online activities of children. Insofar as adults may be tracked, organizations should not use technologies, such as zombie cookies, that make it difficult or impossible for people to opt out.

We provided the following elaboration on the conditions needed for valid opt-out consent:

- Website users must be informed of the purposes for online behavioural advertising, in a manner that is clear, understandable and not buried in a privacy policy. Organizations should consider the most transparent forms of communication with their users, such as online banners, layered approaches and interactive tools,

- Individuals should be informed about these purposes at or before the time of collection, and provided with information about the various parties involved in online behavioural advertising,

- Individuals must be able to opt out of the practice easily. The opt-out provisions should ideally be available at or before the time the information is collected, and take effect immediately. The opt-out should be lasting,

- The personal information that is collected and used should be limited, to the extent practicable, to non-sensitive information. It should thus avoid health and other sensitive information; and

- Information that is collected and used should be destroyed as soon as possible, or transformed in a way that it can no longer identify the particular individual to whom it pertains.

3.7.2 *Guidance on Cloud Computing for SMEs*

Many small and medium-sized enterprises (SMEs) have been flocking to cloud computing solutions, which allow them to rent a slice of the massive computer processing and storage power of a much bigger organization. By adopting cloud-based solutions, organizations effectively leave their IT maintenance and upgrade headaches to someone else.

But SMEs need to know that, for all the apparent benefits of outsourcing their computing to a multinational colossus specializing in such things, there are risks as well. One of those risks is that the SME could lose control of the personal information it collected—information for which it is, ultimately, accountable under PIPEDA.

To help SMEs understand their privacy responsibilities and assess the risks and implications of outsourcing personal information to a cloud-based service, our Office worked with our counterparts in Alberta and British Columbia on new guidance.

Titled *Cloud Computing for Small and Medium-sized Enterprises: Privacy Responsibilities and Consideration*, the guidance reminds businesses, regardless of their size, that they are ultimately accountable for the personal information they collect, use and disclose, even if the personal information is outsourced to a cloud-based service provider.

Cloud Computing for Small and Medium-sized Enterprises: Privacy Responsibilities and Consideration (http://www.priv.gc.ca/information/pub/gd_cc_201206_e.asp)

The document equips SMEs with a series of questions they should consider when shopping for a cloud computing solution for their business. It recommends that SMEs perform careful assessments and use contractual or other means to ensure that personal information is appropriately handled and protected by the cloud provider.

In particular, the guidance cautions against "take it or leave it" contracts, which may allow for more liberal usage of personal information and retention practices, or contain standard clauses that may not be sufficient for SMEs to meet their privacy obligations.

The document also prompts SMEs to think about security safeguards, such as encryption and access controls, and to consider how the law applies in different jurisdictions.

Transparency is key, so SMEs are encouraged not only to understand their responsibilities, but also to ensure that they meet customers' expectations.

3.7.3 *Privacy Emergency Kit*

Laws governing the collection, use and disclosure of personal information exist at all levels of government, for both the public and the private sectors. All of them permit the appropriate sharing of personal information in the event of an emergency—a fact that is often misunderstood in times of stress and urgency.

During a time of disaster, some organizations that are subject to PIPEDA may be asked to give authorities personal information of clients or customers, without the consent of the individuals concerned. For example, an airline or a dentist office could be asked for personal information to help emergency responders determine whether people are missing, or to identify victims.

Over the past year we consulted with our provincial and territorial counterparts in the development of a Privacy Emergency Kit to help organizations handle personal information appropriately before, during and after an emergency.

The kit, released in May 2013, explains that privacy laws should not be considered a barrier to action and the appropriate sharing of information in the event of an emergency. It includes checklists and frequently asked questions about a variety of important issues, such as the legal authorities for sharing personal information.

The guidance was developed in the wake of the *Resolution on Data Protection and Major Natural Disasters*, which was adopted at the 33rd International Conference of Data Protection and Privacy Commissioners in November 2011.

PIPEDA and the Evolution of Privacy Rights

PIPEDA was passed in 2000 and came into force over the subsequent three years. The law has many strengths, including its technologically neutral foundation of principles, which enabled it to adapt to emerging challenges.

In recent years, however, it's become clear that PIPEDA needs some fundamental enhancements to ensure it keeps up with the dramatic changes in the privacy landscape.

One of the most significant threats to personal information lies in the sheer volume of it being held by many global giants of the digital economy. It is becoming increasingly challenging to protect information from unintentional data breaches and sophisticated cyber-criminals.

More and more, organizations are also recognizing the value of the personal information in their hands and are honing their competitiveness through new, sometimes unexpected and even unwelcome uses of the data.

When things go wrong, they can do so on a colossal scale. And when we investigate, we often discover that organizations failed to anticipate the privacy problems they unleashed by rushing their data-intensive new products or services to market.

Worse, when we intervene with recommendations for improvements, the response, all too often, is sluggish—and there's little we can do about it. While companies may in the end agree to recommendations aimed at improving their privacy practices, the process to reach that agreement is often laborious and time-consuming. And ensuring recommendations ultimately get fulfilled is fraught with further expense as the Office lacks legal leverage needed to reach, let alone speed, successful privacy outcomes.

In recent years we have sought to make the most of the Commissioner's existing powers under the law in order to keep up with emerging challenges. We feel we have been relatively effective with those tools, including initiating more complaints, conducting

compliance audits, and exercising our discretion to name names when it is in the public interest to do so.

And yet it has become plain that even this is not enough. The law lacks adequate incentives for organizations to invest in privacy in a significant way, since they can always agree to amend their practices after being investigated or audited, but then not follow through on recommendations – or do so only after considerable hounding over a long period of time. Because the law contains no possibility to order fines or damages, organizations incur few monetary sanctions for noncompliance with PIPEDA —except perhaps the cost of legal counsel or other advisors.

And so we are persuaded that, given the global reach of today's most powerful businesses, Canada needs powers comparable to those in other jurisdictions in order to have the greatest impact on privacy protection.

Indeed, over the past decade, data protection authorities elsewhere have been entrusted with stronger enforcement powers, including the ability to levy significant monetary penalties.

Canada cannot afford to be left behind, with little in the way of consequences for those who do not respect our privacy law. Good privacy practices are key to the consumer confidence that underpins a thriving digital economy.

That is why our Office has advocated for enhanced powers under PIPEDA, including mandatory breach notification, financial consequences for cases of noncompliance, and other changes to the enforcement model.

Stronger enforcement mechanisms would incite companies to promptly address privacy risks and take responsibility for privacy mishaps. Coupled with strengthened accountability requirements, organizations would be encouraged to adopt up-front measures to mitigate risks and ensure compliance with the law.

All this would enable companies to be innovative and competitive, while maintaining consumer trust and confidence in their brand.

This chapter touches on our ongoing efforts to ensure that PIPEDA remains up to today's challenges, and that the Privacy Commissioner is equipped with adequate powers to enforce it.

It also describes our other interactions with Parliament, the institution to which the Privacy Commissioner and her Office are accountable, including a series of hearings into the impact of social media on privacy.

Later in the chapter we highlight our work in the courts, which focused on reinforcing and bolstering organizations' respect for privacy rights and obligations under PIPEDA. This section also includes our Office's appearance before the Supreme Court of Canada, where we advocated for a framework to balance privacy rights and the open-courts principle in the context of teens and social media.

Our efforts in 2012 also extended beyond the federal court and legislative systems to encompass work with provinces and territories, as well as with other international data-protection authorities and related organizations. These, too, are detailed in this chapter.

4.1 IN PARLIAMENT

From the perspective of our Parliamentary Affairs team, 2012 was a busy year. We appeared 10 times before committees of both Houses of Parliament, and submitted three briefs on matters that touched in some way on privacy.

We also analyzed 14 bills to assess their potential impacts on privacy, including Bill C-30, *the Protecting Children from Internet Predators Act*. We identified clear implications for PIPEDA in the bill, because many of its provisions would have interacted with the Act's lawful authority provision. However, by early 2013, the Government had announced it would not proceed with the legislation.

In addition, we answered 57 formal requests from MPs and Senators. Among those, nine were related to PIPEDA. These included three invitations to appear before the Standing Committee on Access to Information, Privacy and Ethics (ETHI) and a briefing session on Bill C-12, *the Safeguarding Canadians' Personal Information Act*. Bill C-12 would amend PIPEDA to introduce breach notification requirements and broaden the grounds under which law enforcement agencies can obtain personal information from organizations.

There were also questions from Parliamentarians about PIPEDA, the use of personal information by tax preparation or credit report companies,

The Privacy Commissioner is an Agent of Parliament, reporting directly to Parliament rather than to the government of the day. Her Office's Parliamentary affairs unit reviews and analyzes legislative initiatives and supports the Commissioner in appearances before Parliament and its relations with Parliamentarians.

U.S. companies using Canadian Social Insurance Numbers to provide services in Canada, and personal information used on websites that could affect the reputations of individuals.

4.1.1 *Commissioner testifies at hearings on social media and privacy*

In May 2012, the Standing Committee on Access to Information, Privacy and Ethics (ETHI) launched an examination into the extent to which social media companies protect the privacy and personal information of Canadians.

The hearings attracted academics, advocates and industry representatives including online giants such as Google, Facebook and Twitter. Commissioner Stoddart, accompanied by Assistant Commissioner Chantal Bernier and staff, was invited to present at the outset of the study, as well as the wrap-up.

The Commissioner offered a framework through which the Committee could focus its study, suggesting that the key challenges to privacy in the context of social media reside in limits on the collection and retention of personal information, ensuring people provide meaningful consent for the collection of their personal information, and accountability for privacy.

She also called on governments, educators and communities to focus on the digital education of Canadians of all ages, including the broader societal and ethical issues raised by new information technologies. Without absolving companies operating on the Internet of their obligations under privacy law, digital literacy helps people understand that the information they post online, about themselves and others, can live on forever.

The Commissioner also said that PIPEDA may need strengthening to encourage compliance and greater accountability, noting an international trend toward stronger enforcement powers among data protection authorities. Currently, the law takes a "soft" approach based on non-binding recommendations, where the biggest risk to an organization's reputation rests in the negative attention that the organization may attract should the Commissioner exercise her power to name it in the public interest.

While most witnesses agreed on the privacy challenges posed by social media, there were differing views on the adequacy of the tools available to address the problems. With the exception of some industry and business representatives, most academics, advocates, one industry association, and provincial Commissioners from British Columbia and Ontario felt the federal Commissioner needed stronger powers.

Witnesses also disagreed on the adequacy of a legislative initiative to make data breach notification mandatory, with some in the business sector arguing such measures would place an undue burden on smaller organizations. The Commissioner, however, disagreed. She argued that, with the vast amounts of personal information held by organizations on increasingly complex platforms, the risk of significant breaches, or of potentially intrusive uses of that information, calls for commensurate safeguards and consequences not currently provided for under PIPEDA.

The Committee's final report was tabled in the House of Commons in April 2013.

4.2 IN THE COURTS

The past year saw several actions at the Federal Court, as well as an appearance before the Supreme Court of Canada. This section describes an application that we brought, as well as applications brought by others, either against us or when we acted as an intervener before the court.

One additional action, involving the youth-oriented social networking site Nexopia, is described in section 1.3 of this report.

4.2.1 *Privacy Commissioner of Canada v. Association of American Medical Colleges* (Federal Court File T-1712-10)

In 2012, our Office brought to a fruitful resolution a Federal Court application that we initiated against the Association of American Medical Colleges (AAMC) in 2010. Our application followed an investigation that we had conducted into the AAMC's practice of collecting the fingerprints and other personal information of candidates writing the Medical College Admission Test (MCAT).

The AAMC owns and administers the MCAT. Through a third-party contractor, the AAMC collected digital fingerprints and other personal information from MCAT candidates. Although the fingerprints were converted into a digital template, the AAMC retained the actual fingerprint images to maintain the integrity of its fingerprint database.

An individual complained to our Office about the AAMC's collection of personal information in connection with the MCAT, alleging that the collection of fingerprints was unnecessary and expressing concern about the retention and safeguarding of the fingerprint data.

Based on the evidence uncovered during our investigation, we concluded that there were less privacy-invasive means to meet the AAMC's purposes.

We also took the view that the AAMC was retaining the personal information it collected for too long and that the association needed to maintain an information-security program and continue to protect information through its contracts with third-party service providers.

The AAMC undertook to make certain changes, including notifying test-takers about the collection of personal information and limiting the retention of the personal information it collected on each test day to five years.

The organization also agreed with our recommendations on safeguarding the information collected.

However, the AAMC stated that it would not stop collecting fingerprints from candidates, as well as photographs and a scan of their driver's licences. The organization was of the view that such personal information was necessary to prevent people from fraudulently taking the test on somebody else's behalf.

As a result, the Privacy Commissioner initiated a Federal Court application seeking an order directing the AAMC to find less privacy-intrusive means to ensure the integrity of the examination.

During the course of the application and during mediation discussions, the AAMC presented further evidence and arguments related to the problem of proxy test-taking and other types of exam misconduct, and the need for measures to reduce the risk of fraud.

Our Office was ultimately satisfied that the evidence showed that a serious and significant risk of fraud existed in the context of the administration of the MCAT exam, and that the AAMC had justified its collection and use of a limited amount of personal information for the purposes of protecting the integrity of the MCAT, guarding against proxy testing, and investigating misconduct during the MCAT exam.

Our Office and the AAMC agreed to a resolution that resulted in a settlement of the issues raised in the application.

The AAMC agreed to limit the personal information it collects, and to cease recording personal information from government identification documents presented to confirm a test taker's identity.

The association also agreed to collect and retain fingerprint information only in digital format. All digital fingerprint images collected will be converted into unique digital templates and securely stored. As well, the personal information collected from test takers will be retained for a maximum of five years.

Our Office was satisfied that this outcome effectively addressed concerns with respect to both privacy and AAMC's need to protect the integrity of the high-stakes MCAT exam.

4.2.2 *X v. The Toronto-Dominion Bank et al* (Federal Court File No. T-2123-11)

Two individuals complained to our Office that the Toronto Dominion Bank had provided a Mortgage Information Only statement to lawyers acting for a company recovering a debt from the individuals on two separate occasions in 2003 and 2008.

Following an investigation, the Assistant Privacy Commissioner found that the bank had disclosed the complainants' personal information in 2003 without consent, and that this aspect of the complaint was well founded.

The Assistant Commissioner found no evidence that the bank was involved in the second disclosure in 2008. The bank agreed to retrain its employees and to remind them of the importance of maintaining customer confidentiality.

On Dec. 30, 2011, the complainants filed a Notice of Application in Federal Court pursuant to s. 14 of PIPEDA, seeking damages against the bank for its actions. The bank brought a motion to strike the application on the grounds that it was barred by the operation of an Alberta statute of limitations.

On May 1, 2012, the Privacy Commissioner was granted leave to be added as a party to the proceeding to address the issues raised by the bank's motion to strike. However, on Sept. 12, 2012, the complainants and the bank reached a settlement and the application was dismissed.

4.2.3 Judicial review applications: *X v. Privacy Commissioner of Canada* (Federal Court File No. T-1587-11 and T-1588-11)

An individual had complained to our Office that his former employer's counselling service provider had disclosed personal information to the individual's employer, who in turn disclosed the information to other employees as well as the person's physician and an independent medical examiner.

Our investigation found that the complaints were not well founded and reported on this matter in last year's Annual Report.

On Sept. 27, 2011, the complainant brought two applications for judicial review of two Reports of Findings issued by our Office with respect to his complaints. The applicant alleged that the Commissioner had failed to observe principles of procedural fairness, had based her decision on erroneous findings of fact, and had acted, or failed to act, by reason of fraud or perjured evidence.

On Jan. 15, 2013, the Federal Court dismissed the applications. The Court found that there was no evidence of a breach of procedural fairness and that section 14 of PIPEDA provided the applicant with an adequate alternative remedy in the circumstances. It therefore declined to judicially review the Commissioner's Reports of Findings.

4.2.4 Judicial review application: *X v. The Attorney General of Canada and the Privacy Commissioner of Canada* (Federal Court File No. T-1588-12)

This is a judicial review application relating to our Office's investigation of a complaint alleging that an organization had improperly denied the complainant access to his personal information.

After investigating the complaint, we concluded that the matter was well founded and resolved.

The complainant, however, filed an application for judicial review on Aug. 27, 2012, seeking to have his complaint file reopened.

At the time of the writing of this report, the individual had not filed any affidavit evidence in support of his application, or undertaken any further action in this matter.

4.2.5 Supreme Court of Canada Intervention: *X. v. Bragg Communications Inc.* (Supreme Court of Canada Court File No.34240)

In 2012 our Office sought and was granted leave to intervene in a case before the Supreme Court of Canada that raised a variety of important privacy issues.

The case, brought on behalf of a 15-year-old girl by her father, involved a fake Facebook profile that

an unknown person had created about her. The fake Facebook profile discussed the applicant's physical appearance and alleged sexual activities and preferences.

The applicant obtained the IP address of the account used to publish the fake profile, and applied for a court order requiring the local Internet service provider to disclose the identity of the account holder associated with the IP address in question.

She also sought a confidentiality order that would allow her to proceed by pseudonym, and a partial publication ban to prevent the public from knowing the words contained in the fake Facebook profile.

The trial level court granted the order to disclose the identity of the owner of the IP address in question, but rejected the applicant's request for a confidentiality order and partial publication ban.

This meant that, in order to obtain the information, the applicant would have to give up her anonymity.

Both the Nova Scotia Supreme Court and Court of Appeal denied the applicant's requests for the confidentiality order and partial publication ban, largely because the courts were not satisfied that the applicant had tendered sufficient evidence about the harm she would suffer if the requested relief was not granted.

The applicant ultimately appealed to the Supreme Court of Canada and our Office was granted Intervener status.

The case raised issues that are strategic priorities for our Office, including identity integrity and information technology. It touched on key areas of focus for our Office, including youth privacy, the privacy risks associated with social networking sites, and the need for established social norms and legal rules to adapt to the Internet age.

In written and oral arguments presented before the Court on May 10, 2012, we elaborated on the legal framework that courts should consider when weighing privacy rights against the principle of open courts.

The Supreme Court unanimously granted the appeal in part, holding that the applicant should be allowed to proceed anonymously in her application for an order to disclose the identity of the relevant IP user(s), and that the Courts below had erred in failing to consider the objectively discernible harm to the applicant that would result if her request for anonymity was not granted.

The Supreme Court of Canada held that the interests of privacy and the protection of children from cyberbullying justified restrictions on freedom of the press and open courts.

In their evaluation, granting the applicant anonymity would cause minimal harm to freedom of the press and the open courts principle, compared with the salutary effects of protecting children from online cyberbullying and re-victimization upon publication.

The Court also noted the potentially chilling effect of publication on child victims seeking access to justice.

The Court held, however, that once the applicant's identity was protected, there was no need to grant a publication ban on the other non-identifying information on the Facebook profile, since it could not be linked back to her.

4.3 SUBSTANTIALLY SIMILAR PROVINCIAL AND TERRITORIAL LEGISLATION

Section 25(1) of PIPEDA requires our Office to report annually to Parliament on the "extent to which the provinces have enacted legislation that is substantially similar" to the Act.

Under paragraph 26(2)(b) of PIPEDA, the Governor in Council may issue an Order exempting an organization, a class of organizations, an activity or a class of activities from the application of PIPEDA with respect to the collection, use or disclosure of personal information that occurs within a province that has passed legislation that is "substantially similar" to PIPEDA.

On August 3, 2002 Industry Canada published the *Process for the Determination of 'Substantially Similar' Provincial Legislation by the Governor in Council*, outlining the policy and criteria used to determine whether provincial legislation will be considered substantially similar. Under the policy, laws that are substantially similar:

- provide privacy protection that is consistent with and equivalent to that in PIPEDA;
- incorporate the 10 principles in Schedule 1 of PIPEDA;
- provide for an independent and effective oversight and redress mechanism with powers to investigate; and
- restrict the collection, use and disclosure of personal information to purposes that are appropriate or legitimate.

On Oct. 10, 2012 Newfoundland and Labrador's *Personal Health Information Act* (PHIA) was declared substantially similar to PIPEDA. As a result, personal health information custodians subject to PHIA are exempt from the application of Part 1 of PIPEDA in respect of the collection, use and disclosure of personal health information that occurs in Newfoundland and Labrador. PHIA came into force on April 1, 2011.

Five other provincial laws have previously been declared substantially similar to PIPEDA:

- Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector*;
- British Columbia's *Personal Information Protection Act*;
- Alberta's *Personal Information Protection Act*;
- Ontario's *Personal Health Information Protection Act*, with respect to health information custodians; and
- New Brunswick's *Personal Health Information Privacy and Access Act*, with respect to health information custodians.

4.4 COLLABORATING WITH PROVINCIAL AND TERRITORIAL COUNTERPARTS

We continued in 2012 to work with our provincial and territorial counterparts across Canada on shared issues in privacy compliance. Annual federal/provincial/territorial meetings bring commissioners together to build and support such working relationships.

In late-2011 our Office signed a revised Memorandum of Understanding (MOU) with the Information and Privacy Commissioners of British Columbia and Alberta, fostering further collaboration on private-sector privacy issues.

In signing the MOU, our Offices renewed our commitment to the Private Sector Policy Forum as a means to streamline and support our collaborative efforts. The forum serves as a platform for information exchange and dissemination, which ultimately helps us support organizations with tools, services and knowledge.

In 2012, our three Offices issued three joint publications aimed at private-sector organizations:

- *Getting Accountability Right with a Privacy Management Program* is a guidance document to help private-sector organizations build effective privacy-management programs.
- *Cloud Computing for Small and Medium-sized Enterprises: Privacy Responsibilities and Considerations* explains cloud computing and addresses privacy-related issues such as transparency, security and consent, and
- *Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps* gives mobile application developers tools to understand their privacy-compliance obligations.

We also collaborated with several of our provincial and territorial counterparts in the development of a *"Privacy Emergency Kit,"* guidance to encourage organizations to integrate good practices for handling personal information in the event of an emergency. Several provincial and territorial offices are developing related materials that will be linked from within our guidance.

Please see Chapters 2 and 3 of this report for details on these and other publications.

4.5 GLOBAL INITIATIVES

Recognizing that today's extraordinary advances in information and communication technologies pose unprecedented challenges to the protection of personal information, several states and international organizations have begun to respond to this new reality. Our Office continued to monitor and engage in many aspects of this work.

In January 2012, the European Commission proposed a comprehensive reform of the data protection rules that apply throughout the European Union. Among other things, the proposed reforms would greatly strengthen the enforcement powers of European data protection and privacy commissioners, who would be empowered to fine offending companies up to €1 million, or up to two percent of their annual global revenues.

The Organisation for Economic Co-operation and Development, for its part, is completing a review of its *Guidelines on the Protection of Privacy and Transborder Data Flows*, now more than 30 years old, to determine whether they require revision in light of social and economic changes. Commissioner Stoddart chaired a volunteer expert group that proposed several changes to the Guidelines.

In the United States, President Barack Obama issued *A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, which proposed a Consumer Privacy Bill of Rights for that country. And, after a lengthy review, the Australian government amended its *Privacy Act* to give its commissioner additional powers.

Back in Canada, meanwhile, legislation to implement enhancements to PIPEDA that were recommended by a Parliamentary committee six years ago appears to be stalled and a second mandated review of PIPEDA is overdue.

4.5.1 *Co-operative Enforcement*

As a consequence, the enforcement model provided for under PIPEDA appears increasingly out of date. While we wait for PIPEDA to be amended to include new powers or enforcement tools, one of the ways we have sought to be more effective in this challenging new environment is by working more closely with our international counterparts.

In 2012, our Office entered into written arrangements with the privacy commissioners of Germany and the United Kingdom, which allow us to share information on enforcement matters of mutual interest.

On the strength of a similar arrangement we signed the year before with the Dutch commissioner, 2012 also saw us concluding our first-ever co-ordinated investigation with a foreign data-protection authority. By drawing on the expertise of the Dutch office, we were able to conduct a more thorough and efficient investigation of WhatsApp, a mobile messenger application. The investigation, detailed in section 2.4

of this report, was a valuable learning experience for both offices.

This co-ordinated action was a world first—an international investigation into the privacy practices of a company whose mobile app has an increasingly global following of users.

The effort ultimately led to better privacy practices at WhatsApp and a more privacy-friendly mobile app for millions of Canadians and other users worldwide. It demonstrated that privacy authorities can work together to effect important changes in this increasingly borderless and mobile world.

As one of the co-chairs of a working group tasked with developing a framework and processes to facilitate co-ordinated enforcement actions, the Commissioner also organized an international meeting to discuss ways to overcome barriers to information sharing and to explore potential areas for concerted efforts. The May 2012 meeting in Montreal was attended by the European Data Protection Supervisor and other representatives of data protection and enforcement agencies from Canada, France, Germany, Korea, Mexico, the Netherlands, New Zealand, Poland, the UK, Uruguay and the United States.

The participants also agreed on 10 action items to promote effective co-ordination of enforcement efforts. The *Framework for International Enforcement Co-ordination* was ultimately presented to the 34th International Conference of Data Protection and Privacy Commissioners in Uruguay.

4.5.2. *Other International Activities*

Our Office continues to work with international organizations on a number of other important initiatives to safeguard privacy. Here are summaries of some of the activities we engaged in around the world last year:

- The World Wide Web Consortium, the main international standards organization for the web, set up in 2012 a group of experts to monitor privacy issues affecting the web and to develop standards to address them. Our Office co-chairs this new **Privacy Interest Group** (PING), which expects in the years ahead to explore such issues as: online tracking; location, health and financial data; eGovernment initiatives; online social networking; and identity. PING will also explore broader issues, such as web browser fingerprinting, which can be used to identify users. The creation of an over-arching "Privacy Considerations" document to help standards developers embed privacy principles in their work is one of PING's ongoing efforts.

- Our Office participated in the annual conference of ***L'Association francophone des autorités de protection des données personnelles*** where the Assistant Commissioner made a presentation on the importance of technical expertise for data protection authorities in the evolving digital era. Alongside data protection authorities from France, Switzerland and Quebec, we

successfully proposed that the Canadian Government support an international resolution that would become part of the Kinshasa Declaration, which concluded the XIV *Francophonie* Summit. The resolution recognizes the role of the Internet in promoting human rights, freedom of expression and democratic participation. It also calls for the adoption of binding international rules and of national laws that define the principles of an effective protection of human rights and freedoms when processing personal data.

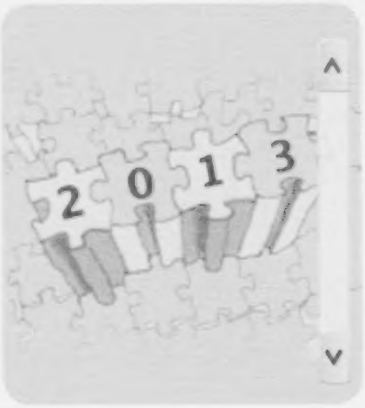
- We continued our work with the **International Working Group on Data Protection in Telecommunications**, better known as the "Berlin Group". Founded in 1983, the organization serves as an early warning system for risks arising from new technological developments. In recent years the organization has tackled a range of topics, such as mobile location information, online voting, telecommunications surveillance, cloud computing, smart metering, electronic micropayments and vehicle event data recorders. The results of the Working Group's deliberations are online in German and English.

- A member of our team represents Canada on a working group of the **International Organization for Standardization** that deals with Identity Management and Privacy Technology. The working group has already published a series of international standards to enhance the security of personal data in biometrics and other practices requiring authentication technologies. Other topics being examined by the group include data protection in cloud computing, identity proofing, privacy impact assessment methodology, secure data deletion and smart grids.

The Year Ahead

As this report makes clear, 2012 was a busy year for our Office. We have every reason to believe that 2013 will be just as busy, and probably significantly more so.

We cannot, for example, expect any of today's threats to privacy to miraculously vanish. If anything, the challenges wrought by technology will only continue to grow.



Moreover, our Office will be moving across the Ottawa River to Gatineau, Que., during the fall, which brings with it the usual tumult and disruption of relocation. We will be joined at our new building by fellow Agents of Parliament —, the Commissioner of Official Languages, Elections Canada and the Office of the Information Commissioner of Canada. In the interests of greater efficiency, our offices will share a library, mail processing room, server room and data centre.

In addition, Commissioner Stoddart's 10 years at the helm of our organization will draw to a close in December, ushering in a period of preparation and transition to the new leadership.

But, to our way of thinking, all this action isn't bad. On the contrary, it makes an organization like ours vibrant and alert. It forces us to critically examine what we do, to ensure that our activities are sensible, relevant and streamlined.

We're not interested in just getting through the day; we want to have an impact on the lives of Canadians—a significant and positive impact.

And that's energizing. Busy, in a word, is good.

Against that backdrop, here's what we have in mind for 2013:

Legislative reform

The environment in which personal information is collected, used and disclosed has undergone a dramatic reshaping since PIPEDA was passed. With the astonishing capability of modern computers to collect, store, manipulate and interpret data, personal information has become a red-hot commodity.

The new technology has resulted in exciting new products and services for consumers. But it's not without risk, including the loss, theft or misappropriation of people's personal information.

In spite of the best efforts of our Office to encourage organizations to report data breaches, we still don't know how prevalent such spills actually are. Indeed, while Parliament continues to consider a bill to make breach notification mandatory, the perverse truth is that companies that don't report such incidents enjoy a competitive advantage over the accountable ones that do.

We've also hit snags in our efforts to ensure that organizations that we've investigated actually implement the changes they promise. During investigations, we have frequently noticed that privacy protections have not been built into products and services. We then encounter practical issues around ensuring that organizations take accountability for any follow-up actions that they agree to at the end of an investigation.

Such actions typically take longer than the amount of time allotted under the law to go to Federal Court to have the Commissioner's recommendations enforced. This has made it challenging to ensure that appropriate changes are made to address problems.

In another shortcoming in the existing law, we have no way to determine how often organizations are compelled to disclose the personal information of clients or customers at the request of police or other law enforcement officials. The disclosure of such information can have significant ramifications for individuals, but the veil over these disclosures is opaque and absolute.

PIPEDA is a principles-based law, which gives it strength and flexibility. Even so, we've concluded that incentives are needed to ensure that organizations are building privacy protections into their products and services from the start.

That is why we want to see stronger enforcement powers, such as the power to make orders and impose financial consequences for ongoing violations of the Act. We'd also like to see mandatory breach reporting, public reporting on disclosures without the knowledge or consent of individuals under the "lawful authority" provision, and enhanced accountability requirements for organizations.

We will continue in 2013 to push for the necessary changes to PIPEDA and other laws, in order to ensure that Canadians' personal information is protected and their trust secured in this complex and burgeoning digital economy.

We have been concerned about Bill C-12, *the Safeguarding Canadians' Personal Information Act*, which would amend PIPEDA to introduce breach notification requirements and broaden the grounds under which law enforcement agencies could obtain personal information from organizations. At the time of writing, the bill, introduced in the House of Commons in September 2011, had not yet been debated.

Complaints and Inquiries

Handling the information requests and privacy complaints of Canadians remain among our core responsibilities, and we will continue to search for ways to maximize our impact in this regard.

We will continue to improve and streamline our processes with an eye to further speeding up our response times. Watch for greater emphasis at the front end, with more active involvement from our Information Centre and Intake Unit, and a concerted effort to resolve issues through our Early Resolution process.

We'll also be piloting a new mediation process that will aim to bring parties to a quick agreement and a commitment to abide by it. We will continue to focus our investigative resources on areas representing the top privacy risks to Canadians, especially when we select Commissioner-initiated complaints.

And we'll continue to promote voluntary compliance, encouraging organizations to address complaints before we issue our final reports.

A more timely and effective complaint-handling process is good for complainants as well as respondent organizations. And it's good for Canadians as a whole, because every resolved case contributes to enhanced privacy protections for everyone.

Canada's Anti-Spam Legislation

Meantime, our PIPEDA Investigations Branch is continuing to gear up for the increased complaint load we expect from the passage of Canada's anti-spam law (CASL), which gained Royal Assent on Dec. 15, 2010. At the time of this report's publication, CASL's regulations were yet to be finalized and it was yet to be determined when the legislation would come into force.

In the meantime we are working with our partner agencies—the CRTC and the Competition Bureau—with which we will share investigative responsibilities under the new law.

And we're boosting our technological capacity, so that our investigators will be properly trained to look into complaints over the unauthorized collection of personal information through electronic address harvesting and spyware.

Research and Policy Guidance

In the year ahead, our Office will continue our proactive approach toward the identification and exploration of emerging privacy challenges. Our in-house research efforts bolster the expertise of our own staff, and strengthen the guidance we issue to business and other stakeholders.

We already have our eyes on several important topics, including mobile payments, facial recognition software, and the best ways to obtain consent for the collection of personal information in the online environment.

Another particularly challenging topic to come under our scrutiny are so-called "revenge" websites, which allow people to post offensive and demeaning information and photos about other individuals, often ex-spouses or romantic partners. Revenge websites have been refusing requests from targeted individuals to take down photos and comments, and these people are turning to us for protection under the privacy law. In the coming year, our Office will be preparing and sharing a research paper that will examine this issue and its privacy implications.

Collaboration with other data protection authorities

As we have done for some years, we will continue to work with our provincial and territorial counterparts on joint investigations and the development of guidance.

Likewise, we will continue to forge effective relationships with our international counterparts to investigate or otherwise address issues of common concern. We are persuaded that this is the most sensible way to strengthen protections for personal information in our interconnected world.

Of particular note, 2013 will see the inaugural Global Privacy Enforcement Network (GPEN) Internet Privacy "Sweep." An initiative spearheaded by our Office, the Sweep brings together privacy enforcement authorities from around the world in a co-ordinated effort to identify potential commercial privacy issues and trends. In this, the first year of the initiative, more than a dozen international and Canadian privacy authorities are turning the spotlight on the transparency of organizations' privacy practices. Our Office will play the co-ordinating role for this year.

Appendix 1

Definitions

DEFINITIONS OF COMPLAINT TYPES UNDER PIPEDA

Complaints received by the OPC are categorized according to the principles and provisions of PIPEDA that are alleged to have been contravened:

Access: An individual has been denied access to his or her personal information by an organization, or has not received all the personal information, either because some documents or information are missing or because the organization has applied exemptions to withhold information.

Accountability: An organization has failed to exercise responsibility for personal information in its possession or custody, or has failed to identify an individual responsible for overseeing its compliance with the Act.

Accuracy: An organization has failed to ensure that the personal information it uses is accurate, complete, and up-to-date.

Challenging compliance: An organization has failed to put procedures or policies in place that allow an individual to challenge its compliance with the Act, or has failed to follow its own procedures and policies.

Collection: An organization has collected personal information that is not necessary, or has collected it by unfair or unlawful means.

Consent: An organization has collected, used or disclosed personal information without meaningful consent, or has made the provision of a good or service conditional on individuals consenting to an unreasonable collection, use, or disclosure.

Correction/Notation: The organization has failed to correct personal information as requested by an individual, or, where it disagrees with the requested correction, has not placed a notation on the information indicating the substance of the disagreement.

Fee: An organization has required more than a minimal fee for providing individuals with access to their personal information.

Openness: An organization has failed to make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Retention: Personal information is retained longer than necessary for the fulfillment of the purposes that an organization stated when it collected the information, or, if it has been used to make a decision about an individual, has not been retained long enough to allow the individual access to the information.

Safeguards: An organization has failed to protect personal information with appropriate security safeguards.

Time limits: An organization has failed to provide an individual with access to his or her personal information within the time limits set out in the Act.

Use and disclosure: Personal information is used or disclosed for purposes other than those for which it was collected, without the consent of the individual, and the use or disclosure without consent is not one of the permitted exceptions in the Act.

DEFINITIONS OF FINDINGS AND OTHER DISPOSITIONS

At the beginning of 2012, our Office altered some of the definitions of findings and dispositions so that they would better convey the outcomes of our investigations under PIPEDA. These goal of the new dispositions was also to better reflect the responsibilities of organizations to demonstrate accountability under the Act.

The definitions below explain what each disposition means.

Not well founded: The investigation uncovered no or insufficient evidence to conclude that an organization contravened PIPEDA.

Well founded and conditionally resolved: The Commissioner determined that an organization contravened a provision of PIPEDA. The organization committed to implementing the recommendations made by the Commissioner and demonstrating their implementation within the time frame specified.

Well founded and resolved: The Commissioner determined that an organization contravened a provision of PIPEDA. The organization demonstrated it had taken satisfactory corrective action to remedy the situation, either proactively or in response to recommendations made by the Commissioner, by the time the finding was issued.

Well founded: The Commissioner determined that an organization contravened a provision of PIPEDA.

Early resolved: The OPC helped negotiate a solution that satisfied all involved parties, without a formal investigation being undertaken. The Commissioner does not issue a report.

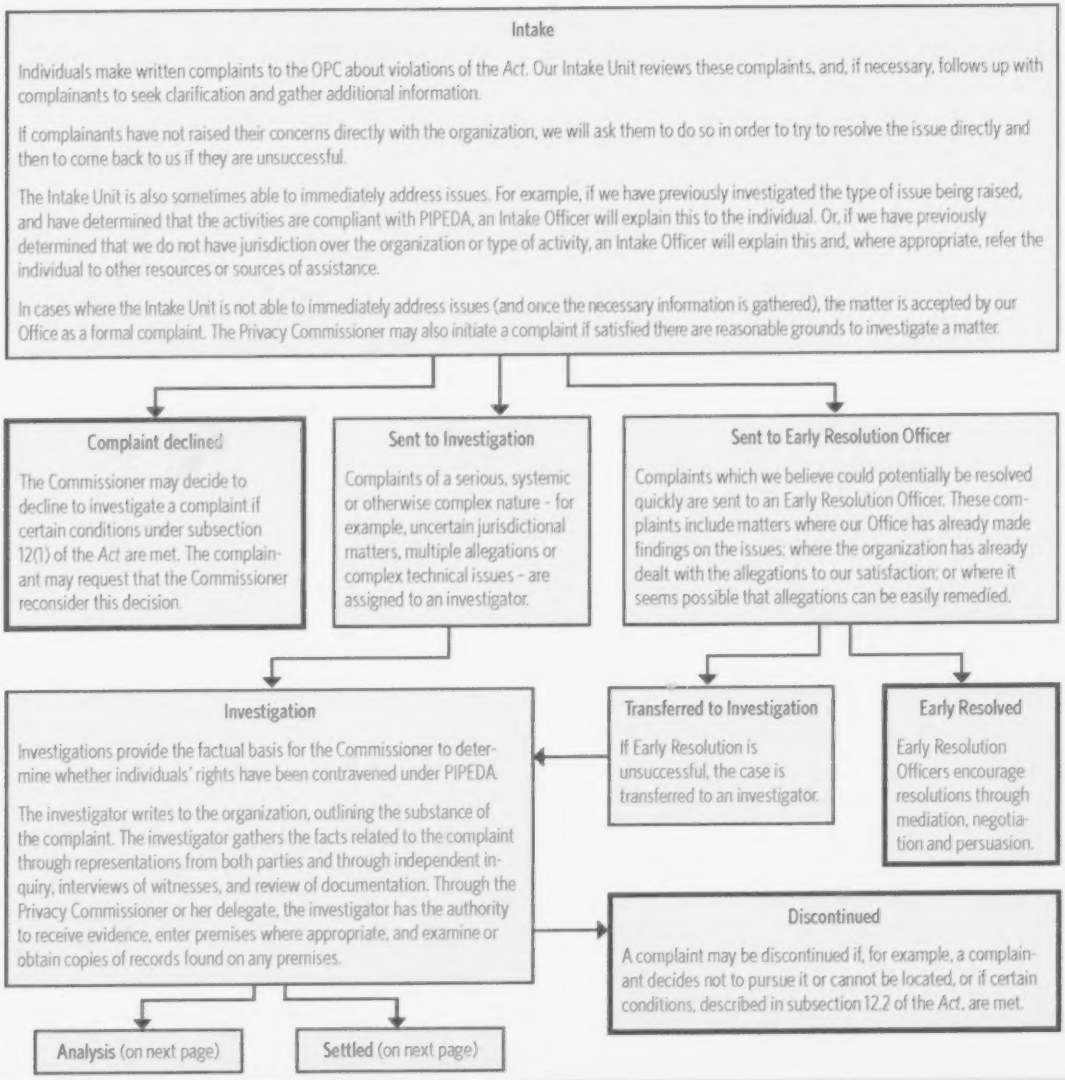
Settled: The OPC helped negotiate a solution that satisfied all involved parties during the course of the investigation. The Commissioner does not issue a report.

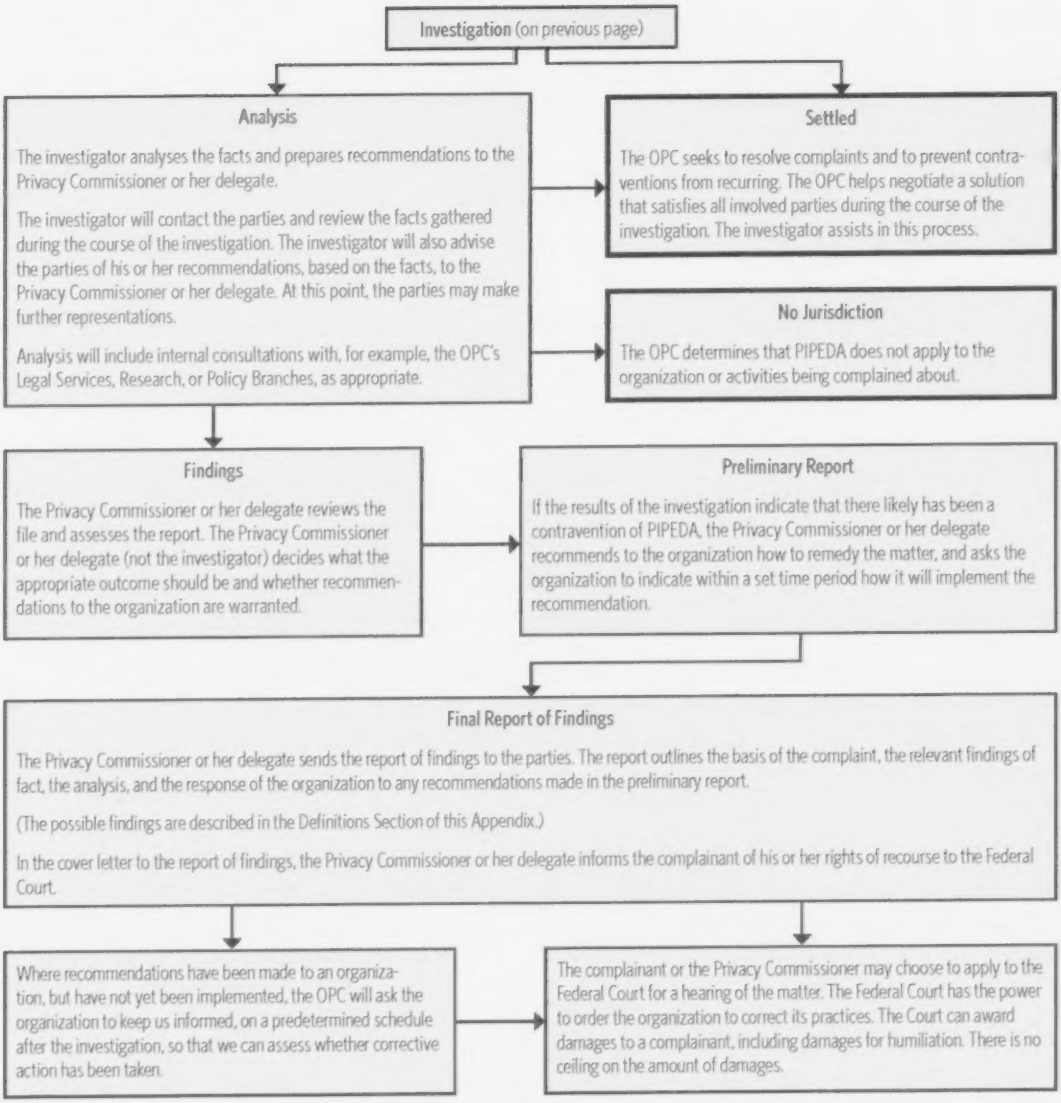
Discontinued: The investigation was discontinued before the allegations were fully investigated. An investigation may be discontinued at the Commissioner's discretion for the reasons set out in subsection 12.2(1) of PIPEDA, as a result of a request by the complainant, or where the complaint has been abandoned.

Declined to Investigate: The Commissioner declined to commence an investigation in respect of a complaint because the Commissioner was of the view that the complainant ought first to exhaust grievance or review procedures otherwise reasonably available; the complaint could be more appropriately dealt with by means of another procedure provided for under the laws of Canada or of a province; or, the complaint was not filed within a reasonable period after the day on which the subject matter of the complaint arose, as set out in subsection 12(1) of PIPEDA.

No jurisdiction: Based on the preliminary information gathered, it was determined that PIPEDA did not apply to the organization or activity that was the subject of the complaint. The Commissioner does not issue a report.

INVESTIGATION PROCESS


Intake
Individuals make written complaints to the OPC about violations of the Act. Our Intake Unit reviews these complaints, and, if necessary, follows up with complainants to seek clarification and gather additional information.
If complainants have not raised their concerns directly with the organization, we will ask them to do so in order to try to resolve the issue directly and then to come back to us if they are unsuccessful.
The Intake Unit is also sometimes able to immediately address issues. For example, if we have previously investigated the type of issue being raised, and have determined that the activities are compliant with PIPEDA, an Intake Officer will explain this to the individual. Or, if we have previously determined that we do not have jurisdiction over the organization or type of activity, an Intake Officer will explain this and, where appropriate, refer the individual to other resources or sources of assistance.
In cases where the Intake Unit is not able to immediately address issues (and once the necessary information is gathered), the matter is accepted by our Office as a formal complaint. The Privacy Commissioner may also initiate a complaint if satisfied there are reasonable grounds to investigate a matter.
Complaint declined
The Commissioner may decide to decline to investigate a complaint if certain conditions under subsection 12(1) of the Act are met. The complainant may request that the Commissioner reconsider this decision.
Sent to Investigation
Complaints of a serious, systemic or otherwise complex nature - for example, uncertain jurisdictional matters, multiple allegations or complex technical issues - are assigned to an investigator.
Sent to Early Resolution Officer
Complaints which we believe could potentially be resolved quickly are sent to an Early Resolution Officer. These complaints include matters where our Office has already made findings on the issues; where the organization has already dealt with the allegations to our satisfaction; or where it seems possible that allegations can be easily remedied.
Investigation
Investigations provide the factual basis for the Commissioner to determine whether individuals' rights have been contravened under PIPEDA.
The investigator writes to the organization, outlining the substance of the complaint. The investigator gathers the facts related to the complaint through representations from both parties and through independent inquiry, interviews of witnesses, and review of documentation. Through the Privacy Commissioner or her delegate, the investigator has the authority to receive evidence, enter premises where appropriate, and examine or obtain copies of records found on any premises.
Transferred to Investigation
If Early Resolution is unsuccessful, the case is transferred to an investigator.
Early Resolved
Early Resolution Officers encourage resolutions through mediation, negotiation and persuasion.
Discontinued
A complaint may be discontinued if, for example, a complainant decides not to pursue it or cannot be located, or if certain conditions, described in subsection 12.2 of the Act, are met.
Analysis (on next page)
Settled (on next page)


Investigation (on previous page)
Analysis
The investigator analyses the facts and prepares recommendations to the Privacy Commissioner or her delegate.
The investigator will contact the parties and review the facts gathered during the course of the investigation. The investigator will also advise the parties of his or her recommendations, based on the facts, to the Privacy Commissioner or her delegate. At this point, the parties may make further representations.
Analysis will include internal consultations with, for example, the OPC's Legal Services, Research, or Policy Branches, as appropriate.
Settled
The OPC seeks to resolve complaints and to prevent contraventions from recurring. The OPC helps negotiate a solution that satisfies all involved parties during the course of the investigation. The investigator assists in this process.
No Jurisdiction
The OPC determines that PIPEDA does not apply to the organization or activities being complained about.
Findings
The Privacy Commissioner or her delegate reviews the file and assesses the report. The Privacy Commissioner or her delegate (not the investigator) decides what the appropriate outcome should be and whether recommendations to the organization are warranted.
Preliminary Report
If the results of the investigation indicate that there likely has been a contravention of PIPEDA, the Privacy Commissioner or her delegate recommends to the organization how to remedy the matter, and asks the organization to indicate within a set time period how it will implement the recommendation.
Final Report of Findings
The Privacy Commissioner or her delegate sends the report of findings to the parties. The report outlines the basis of the complaint, the relevant findings of fact, the analysis, and the response of the organization to any recommendations made in the preliminary report.
(The possible findings are described in the Definitions Section of this Appendix.)
In the cover letter to the report of findings, the Privacy Commissioner or her delegate informs the complainant of his or her rights of recourse to the Federal Court.
Where recommendations have been made to an organization, but have not yet been implemented, the OPC will ask the organization to keep us informed, on a predetermined schedule after the investigation, so that we can assess whether corrective action has been taken.
The complainant or the Privacy Commissioner may choose to apply to the Federal Court for a hearing of the matter. The Federal Court has the power to order the organization to correct its practices. The Court can award damages to a complainant, including damages for humiliation. There is no ceiling on the amount of damages.

Appendix 2

PIPEDA Investigation Statistics for 2012

COMPLAINTS ACCEPTED BY INDUSTRY SECTOR*

Sector Category	Number	Proportion of all complaints accepted
Financial	49	22%
Services	22	10%
Internet	23	10%
Insurance	15	7%
Sales/Retail	16	7%
Professionals	6	3%
Transportation	11	5%
Telecommunications	23	10%
Accommodations	19	9%
Health	6	3%
Entertainment	7	3%
Other	23	10%
Total	**220**	**100%**

* Industry Sector Categories are defined on the following page.

SECTOR DEFINITIONS:

- **Financial:** Banking, credit intermediation (i.e. credit card issuers, sales financing, consumer lending, loan brokers, financial transactions processing activities), financial investment and related activities, investment and financial planning, monetary authorities.
- **Services:** Civic and professional organizations, personal care services, repair and maintenance services, rewards programs, administrative and support services (includes collection agencies, credit bureaus), educational services, social assistance.
- **Internet:** Data processing, hosting and related services, Internet service providers, social networking, web search portals.
- **Insurance:** Insurance carriers (liability, life and health, property and casualty).
- **Sales/Retail:** Automotive dealers, building materials and suppliers dealers, direct marketing, electronic commerce, retail sales (in-store and online).
- **Professionals:** Accounting, tax preparation, bookkeeping and payroll services, legal services, other professional, scientific and technical services.
- **Transportation:** Air, rail, transit and ground passenger transport, trucks, water transport.
- **Telecommunication:** Mobile applications, satellite telecommunication carriers, telecommunications equipment, wired and wireless telecommunication carriers.
- **Accommodations:** Condominium corporations, cooperative housing, real estate, rental accommodations and traveller accommodations.
- **Health:** Physicians, dentists, pharmacies and other health practitioners
- **Entertainment:** Amusement, gambling and recreation industries and other entertainment services.

COMPLAINTS ACCEPTED BY COMPLAINT TYPE

Complaint Type	Number	Proportion of all complaints accepted
Access	65	30%
Accountability	7	3%
Accuracy	6	3%
Appropriate purposes	2	1%
Challenging Compliance	1	1%
Collection	33	15%
Consent	14	6%
Correction/Notation	10	5%
Fees	1	1%
Identifying Purposes	1	1%
Openness	1	1%
Retention	6	3%
Safeguards	17	8%
Use and Disclosure	56	26%
TOTAL	220	100%*

* Totals may not add up to 100 percent due to rounding.

COMPLAINTS CLOSED BY INDUSTRY SECTOR AND DISPOSITION

Sector Catergory	Early Resolution Cases	Disposition of Investigated Cases										Subtotal of all Investigated cases	Total Early Resolution plus Investigations
		Not Well Founded	No Jurisdiction	Discontinued	Well Founded and Conditionally Resolved	Well Founded and Resolved	Well Founded	Resolved	Settled	Withdrawn	Declined		
Financial	18	9		3		12	3		3	4		34	**52**
Services	10	5				4			9			18	**28**
Internet	8	2	1	1	7	3	1	1	4			20	**28**
Insurance	10	4	1	2	1	4	1		1	6		20	**30**
Sales/Retail	13		1	1		3				1		6	**19**
Professionals	3									1	1	2	**5**
Transportation	10	2		2		5			2			11	**21**
Telecommunications	11	1		2		9				2		14	**25**
Accommodations	16	2	1	2		1			1	1		8	**24**
Health	0		1		1							2	**2**
Entertainment	3				2	2						4	**7**
Other	13		1	1					2	2		6	**19**
Total	115	25	6	14	11	43	5	1	22	17	1	145	**260**

INVESTIGATIONS CLOSED BY COMPLAINT TYPE AND DISPOSITION

	Disposition of Case										
Complaint Type	Not Well Founded	No Jurisdiction	Discontinued	Well Founded and Conditionally Resolved	Well Founded and Resolved	Well founded	Resolved	Settled	Withdrawn	Declined	Total
Use and Disclosure	8	4	5	3	12	4	1	6	4	1	**48**
Access	3	1	4		13			2	5		**28**
Collection	7		2	1	4			3	3		**20**
Consent	3	1		2	6			5	1		**18**
Correction/Notation	3				2			3	1		**9**
Retention	1		1	1		1		1			**5**
Safeguards			1		2			1	1		**5**
Accountability					2			1			**3**
Accuracy									2		**2**
Challenging compliance					1						**1**
Fees					1						**1**
Openness				2							**2**
Identifying purposes				1							**1**
Appropriate purposes			1	1							**2**
Total	**25**	**6**	**14**	**11**	**43**	**5**	**1**	**22**	**17**	**1**	**145**

AVERAGE TREATMENT TIMES BY DISPOSITION

Disposition	Number	Average Treatment Time in Months
Early resolution	115	2.8
Discontinued	14	8.5
No Jurisdiction	6	9.0
Not well-founded	25	14.3
Resolved	1	1.0
Settled	22	10.2
Well-founded	5	17.5
Well-founded conditionally resolved	13	16.4
Well-founded and resolved	41	16.1
Withdrawn	17	5.9
Declined	1	9.0
Total cases	**260**	**—**
Overall Weighted Average	**—**	**8.3**

AVERAGE TREATMENT TIMES BY COMPLAINT AND RESOLUTION TYPES

Complaint Type	Early Resolution Cases		Formal Complaint Investigations	
	Number	Average Treatment Time in Months	Number	Average Treatment Time in Months
Access	38	2.8	29	10.9
Accountability	3	2.5	3	10.6
Accuracy			2	8
Appropriate purposes			2	19
Challenging Compliance	1	2.8	1	12
Collection	25	2.7	20	11.8
Consent	1	1.2	18	14.6
Correction/Notation	5	3.2	9	12
Fees			1	16
Identifying Purposes			1	25
Openness			2	25.5
Retention	5	5.8	5	19.4
Safeguards	8	1.8	5	19.4
Use and Disclosure	29	2.8	47	12
Total Cases	**115**	—	**145**	—
Overall Weighted Average in Months	—	**2.8**	—	**12.6**

VOLUNTARY BREACH NOTIFICATIONS BY INDUSTRY SECTOR AND INCIDENT TYPE

Industry Sector	Incident Type*			Total Incidents per Sector	Proportion of all Incidents
	Accidental disclosure	Loss	Unauthorized access, use or disclosure		
Financial	4	2	13	19	58%
Services			1	1	3%
Insurance	2			2	6%
Sales/Retail					
Telecommunications			3	3	9%
Internet			1	1	3%
Entertainment	1		2	3	9%
Accommodations	1		1	2	6%
Other		1		1	3%
Health					
Professionals	1			1	3%
Transportation					
Total	**9**	**3**	**21**	**33**	100%

* See definitions below

Definitions of Data Breach Types:

Accidental disclosure: Incidents where an organization discloses personal information to unintended recipients by accident. For example, bank statements sent to the wrong address through mechanical or human error, or personal information made publicly available on an organization's website through a technical error.

Loss: Incidents where personal information is lost by an organization, usually through the loss of a laptop, CD or paper documents.

Unauthorized access, use or disclosure: Incidents where personal information is accessed, used or disclosed by someone without an organization's authorization. For example, a stolen laptop, an online hack of an organization's database, or an employee accessing or using personal information for unauthorized purposes.